UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

PATCO CONSTRUCTION COMPANY, INC.,	)	
Plaintiff	)	
v.	)	***No. 2:09-cv-503-DBH***
PEOPLE'S UNITED BANK d/b/a OCEAN BANK,	)	
Defendant	)	

RECOMMENDED DECISION ON CROSS-MOTIONS FOR SUMMARY JUDGMENT

Defendant People's United Bank d/b/a Ocean Bank ("Ocean Bank" or "Bank") moves for summary judgment as to all six counts of the operative complaint of Patco Construction Company, Inc. ("Patco"), and Patco cross-moves for summary judgment as to Count I. *See* Defendant People's United Bank's Motion for Summary Judgment ("Defendant's S/J Motion") (Docket No. 62) at 1; Plaintiff's Motion for Summary Judgment ("Plaintiff's S/J Motion") (Docket No. 74) at 1. Ocean Bank also moves to exclude the expert testimony of George F. Thomas and to strike Patco's jury demand, while Patco moves to exclude in part the expert testimony of Peter A. Makohon. *See* Defendant People's United Bank's *Daubert*/*Kumho* Motion To Exclude Expert Testimony of George F. Thomas ("Defendant's Motion To Exclude") (Docket No. 64); Defendant People's United Bank's Motion To Strike Plaintiff's Jury Trial Demand ("Defendant's Motion To Strike") (Docket No. 66); Plaintiff's Motion To Exclude Certain Testimony of Peter A. Makohon ("Plaintiff's Motion To Exclude") (Docket No. 77).

For the reasons that follow, I recommend that the court grant Ocean Bank's motion for summary judgment as to all counts of Patco's operative Second Amended Complaint and deny Patco's cross-motion for summary judgment as to Count I. This disposition, if adopted by the

court, would moot the parties' motions to exclude expert testimony and the Bank's motion to strike Patco's jury trial demand. Hence, I do not consider the latter three motions.

I. Applicable Legal Standards

A. Federal Rule of Civil Procedure 56

Summary judgment is appropriate "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); *Santoni v. Potter*, 369 F.3d 594, 598 (1st Cir. 2004). "A dispute is genuine if the evidence about the fact is such that a reasonable jury could resolve the point in the favor of the non-moving party." *Rodríguez-Rivera v. Federico Trilla Reg'l Hosp. of Carolina*, 532 F.3d 28, 30 (1st Cir. 2008) (quoting *Thompson v. Coca-Cola Co.*, 522 F.3d 168, 175 (1st Cir. 2008)). "A fact is material if it has the potential of determining the outcome of the litigation." *Id.* (quoting *Maymi v. P.R. Ports Auth.*, 515 F.3d 20, 25 (1st Cir. 2008)).

The party moving for summary judgment must demonstrate an absence of evidence to support the nonmoving party's case. *Celotex Corp. v. Catrett*, 477 U.S. 317, 325 (1986). In determining whether this burden is met, the court must view the record in the light most favorable to the nonmoving party and give that party the benefit of all reasonable inferences in its favor. *Santoni*, 369 F.3d at 598. Once the moving party has made a preliminary showing that no genuine issue of material fact exists, the nonmovant must "produce specific facts, in suitable evidentiary form, to establish the presence of a trialworthy issue." *Triangle Trading Co. v. Robroy Indus., Inc.*, 200 F.3d 1, 2 (1st Cir. 1999) (citation and internal punctuation omitted); Fed. R. Civ. P. 56(c). "As to any essential factual element of its claim on which the nonmovant would bear the burden of proof at trial, its failure to come forward with sufficient evidence to generate a trialworthy issue warrants summary judgment to the moving party." *In re Spigel*, 260

F.3d 27, 31 (1st Cir. 2001) (citation and internal punctuation omitted).

"This framework is not altered by the presence of cross-motions for summary judgment." *Cochran v. Quest Software, Inc.*, 328 F.3d 1, 6 (1st Cir. 2003). "[T]he court must mull each motion separately, drawing inferences against each movant in turn." *Id.* (citation omitted); *see also, e.g., Wightman v. Springfield Terminal Ry. Co.*, 100 F.3d 228, 230 (1st Cir. 1996) ("Cross motions for summary judgment neither alter the basic Rule 56 standard, nor warrant the grant of summary judgment *per se.* Cross motions simply require us to determine whether either of the parties deserves judgment as a matter of law on facts that are not disputed. As always, we resolve all factual disputes and any competing, rational inferences in the light most favorable to the [nonmovant].") (citations omitted).

B. Local Rule 56

The evidence that the court may consider in deciding whether genuine issues of material fact exist for purposes of summary judgment is circumscribed by the local rules of this district. *See* Loc. R. 56. The moving party must first file a statement of material facts that it claims are not in dispute. *See* Loc. R. 56(b). Each fact must be set forth in a numbered paragraph and supported by a specific record citation. *See id.* The nonmoving party must then submit a responsive "separate, short, and concise" statement of material facts in which it must "admit, deny or qualify the facts by reference to each numbered paragraph of the moving party's statement of material facts[.]" Loc. R. 56(c). The nonmovant likewise must support each denial or qualification with an appropriate record citation. *See id.* The nonmoving party may also submit its own additional statement of material facts that it contends are not in dispute, each supported by a specific record citation. *See id.* The movant then must respond to the nonmoving party's statement of additional facts, if any, by way of a reply statement of material facts in

which it must "admit, deny or qualify such additional facts by reference to the numbered paragraphs" of the nonmovant's statement. *See* Loc. R. 56(d). Again, each denial or qualification must be supported by an appropriate record citation. *See id.*

Failure to comply with Local Rule 56 can result in serious consequences. "Facts contained in a supporting or opposing statement of material facts, if supported by record citations as required by this rule, shall be deemed admitted unless properly controverted." Loc. R. 56(f). In addition, "[t]he court may disregard any statement of fact not supported by a specific citation to record material properly considered on summary judgment" and has "no independent duty to search or consider any part of the record not specifically referenced in the parties' separate statement of fact." *Id.*; *see also, e.g., Sánchez-Figueroa v. Banco Popular de P.R.*, 527 F.3d 209, 213-14 (1st Cir. 2008); Fed. R. Civ. P. 56(e)(2) ("If a party fails to properly support an assertion of fact or fails to properly address another party's assertion of fact as required by Rule 56(c), the court may . . . consider the fact undisputed for purposes of the motion[.]").

II. Factual Background

The parties' statements of material facts, credited to the extent either admitted or supported by record citations in accordance with Local Rule 56, reveal the following relevant facts.[1]

A. The Parties

Patco is a family-owned second generation commercial, industrial, and residential developer and contractor located in Sanford, Maine. Plaintiff's Statement of Undisputed Material Facts ("Plaintiff's SMF") (Docket No. 75) ¶ 1; Defendant People['s] United Bank's Opposition to Plaintiff's Statement of Undisputed Material Facts ("Defendant's Opposing SMF")

[1] To the extent that I have incorporated one of the party's qualifications into the statement of the other, I have determined that the qualification is supported by the record citation(s) given.

(Docket No. 90) ¶ 1. Patco has been in business since 1985 and has built more than 300 commercial buildings and 400 residences. Statement of Material Facts in Support of Defendant People's United Bank's Motion for Summary Judgment ("Defendant's SMF") (Docket No. 67) ¶ 2; Plaintiff's Opposing Statement of Material Facts and Statement of Additional Material Facts ("Plaintiff's Opposing SMF") (Docket No. 100) ¶ 2. Patco's gross revenues, at their peak in 2005, were between $17 million and $18 million. *Id.* ¶ 3.[2]

When Patco first began banking with Ocean Bank, then Ocean National Bank, in 1985, Ocean Bank was an independent southern Maine-based community bank. Plaintiff's SMF ¶ 2; Defendant's Opposing SMF ¶ 2. Ocean Bank was later acquired by the Chittenden family of banks, based in Burlington, Vermont. *Id.* ¶ 3. The Chittenden banks, including Ocean Bank, subsequently became a division of People's United Bank, a regional bank based in Bridgeport, Connecticut. *Id.* ¶ 4. People's United Bank operates other local banks such as Maine Bank & Trust, where Patco also had an account in May 2009. *Id.* ¶ 5. Ocean Bank was a division of People's United Bank at the time that the allegedly unauthorized withdrawals at issue in this case occurred. *Id.* ¶ 6.

Ocean Bank permits its commercial customers to make electronic funds transfers *via* online banking, referred to at Ocean Bank as "eBanking." Defendant's SMF ¶ 5; Plaintiff's Opposing SMF ¶ 5. Ocean Bank allows its eBanking commercial customers to make electronic funds transfers through Ocean Bank via the Automated Clearing House ("ACH") network, a system used by banks to transfer funds electronically between accounts. *Id.* ¶ 6.

In or about September 2003, Patco added eBanking for Business to its account. *Id.* ¶ 8. Patco used eBanking primarily to make weekly payroll payments to certain employees through

[2] My recitation incorporates, in relevant part, Patco's qualification.

the ACH network. Plaintiff's SMF ¶ 9; Defendant's Opposing SMF ¶ 9. These transactions were always initiated from one of several computers housed at Patco's offices in Sanford, Maine, and originated from a single static Internet Protocol ("IP") address. *Id.* ¶ 12.[3] Each payroll transaction was accompanied by weekly ACH withdrawals for federal and state tax withholding as well as 401(k) contributions. *Id.* ¶ 13. Patco also used eBanking to transfer money from the accounts of Patco and related entities at Maine Bank & Trust, which maintains a branch in Sanford, Maine, into its Ocean Bank checking account. *Id.* ¶ 14.[4]

Beginning on May 7, 2009, unknown third parties initiated a series of withdrawals from Patco's account over the course of several days. Defendant's SMF ¶¶ 183-87; Plaintiff's Opposing SMF ¶¶ 183-87. The withdrawals totaled $588,851. *Id.* ¶ 188. Of this amount, Ocean Bank blocked $243,406 of the transfers. *Id.* ¶ 189.

B. The Parties' Agreements

In September 2003, Patco entered into the following agreements with Ocean Bank: the eBanking for Business Agreement ("Original eBanking Agreement"), the Ocean Bank Automated Clearing House Agreement ("ACH Agreement"), and the Investment and Line of Credit Sweep Account (Managed Balance Agency Agreement) ("Sweep Agreement"). *Id.* ¶ 10.

[3] Ocean Bank qualifies this statement, asserting that Patco's ACH transactions made from February 13, 2009, through May 6, 2009, originated from a single IP address, and no information regarding the IP address used by Patco for ACH transactions is available outside of this time period because the logs go back only 90 days. Defendant's Opposing SMF ¶ 12; Supplemental Declaration of Jeffrey R. Tarte in Support of Defendant People's United Bank's Opposition to Plaintiff Patco Construction Company, Inc.'s Motion for Summary Judgment ("Suppl. Tarte Decl.") (Docket No. 93), Tab 1 to Defendant People's United Bank's Master Supplemental Appendix in Support of Its Oppositions to Plaintiff's Motions for Summary Judgment & To Exclude Certain Testimony of Peter A. Makohon ("Suppl. Appendix") (Docket No. 93), ¶ 6.

[4] Patco states that its transfers between Maine Bank & Trust and Ocean Bank stopped in 2008, Plaintiff's SMF ¶ 14, but Ocean Bank denies this, stating that its log reflects an ACH transfer from Patco's Maine Bank & Trust account to its Ocean Bank checking account in the amount of $204,724 on March 3, 2009, Defendant's Opposing SMF ¶ 14; Suppl. Tarte Decl. ¶ 9.

1. Original eBanking Agreement

On February 3, 2004, Ocean Bank sent a copy of the Original eBanking Agreement to Patco. *Id.* ¶ 11. The cover letter enclosing the Original eBanking Agreement stated: "Please familiarize yourself with the *eBanking for Business Agreement*. . . . If you have any questions, check the user guide online or the screen-by-screen icons." *Id.* ¶ 12 (emphasis in original).[5] Thomas McDowell, Patco's Chief Financial Officer, could not recall ever checking the user guide online. *Id.* ¶ 13.

Patco distributed a copy of the Original eBanking Agreement internally and required Patco employees McDowell, Vickie Kelly, Diana Pierce, Angie Pelham, Mike Patterson, Greg Patterson, and Mark Patterson to read and initial the Original eBanking Agreement. *Id.* ¶ 14.[6] McDowell identified this agreement and was among the individuals who wrote the date of review next to his name. *Id.* ¶ 15.[7] Mark Patterson, Patco's co-owner and Treasurer, reviewed the Original eBanking Agreement on or about September 30, 2003, and wrote the date of his review next to his name. *Id.* ¶ 16.[8] McDowell acknowledged that Patco accepted the terms and conditions of the Original eBanking Agreement when it logged into eBanking. *Id.* ¶ 18.

The Original eBanking Agreement stated that "use of the *Ocean National Bank's eBanking for Business* password constitutes authentication of all transactions performed by you or on your behalf." *Id.* ¶ 19 (emphasis in original).[9] The Original eBanking Agreement stated that Ocean Bank did not "assume[] any responsibilities" with respect to Patco's use of eBanking,

[5] My recitation incorporates Patco's qualification (mischaracterized as a denial).
[6] Patco qualifies this statement, asserting that employees did not initial the document but, rather, wrote the date of their review next to their name, and Mike Patterson did not review it. Plaintiff's Opposing SMF ¶ 14; Original eBanking Agreement (Docket No. 68), Tab 1A to Defendant People's United Bank's Master Appendix in Support of Its Motions for Summary Judgment, To Strike Plaintiff's Jury Trial Demand, & *Daubert*/*Kumho* Motion To Exclude Expert Testimony of George F. Thomas ("Appendix") (Docket No. 68), at 6672.
[7] My recitation incorporates Patco's qualification.
[8] My recitation incorporates Patco's qualification.
[9] My recitation incorporates Patco's qualification.

that "electronic transmission of confidential business and sensitive personal information" was at Patco's risk, and that Ocean Bank was liable only for its gross negligence, limited to six months of fees. *Id.* ¶ 20.[10] The Original eBanking Agreement also provided that "use of *Ocean National Bank's eBanking for Business* by any one owner of a joint account or by an authorized signor on an account, shall be deemed an authorized transaction on an account unless you provide us with written notice that the use of *Ocean National Bank's eBanking for Business* is terminated or that the joint account owner or authorized signor has been validly removed form [sic] the account." *Id.* ¶ 22 (emphasis in original).[11] McDowell admitted that he understood what this provision meant in 2004. *Id.* ¶ 23.

The Original eBanking Agreement stated: "We reserve the right to modify these terms and conditions at any time effective upon publication." *Id.* ¶ 24.[12] The Original eBanking Agreement also provided: "You are responsible for all transfers you authorize using *Ocean National Bank's eBanking for Business*." *Id.* ¶ 25 (emphasis in original).[13] The Original eBanking Agreement provided in three separate sections that Patco had to contact Ocean Bank immediately when it discovered an unauthorized transaction. *Id.* ¶ 26.

2. Modified eBanking Agreement

Ocean Bank modified the Original eBanking Agreement and published the eBanking Agreement on the Bank's website. Defendant's SMF ¶ 28; Declaration of Jeffrey R. Tarte in Support of Defendant People's United Bank's Motion for Summary Judgment ("Tarte Decl.") (Docket No. 68), Tab 1 to Appendix, ¶ 10.[14] The Modified eBanking Agreement had been

[10] My recitation incorporates, in part, Patco's qualification.
[11] My recitation incorporates Patco's qualification.
[12] I omit the word "clearly," sustaining Patco's objection, Plaintiff's Opposing SMF ¶ 24, that it is argumentative.
[13] My recitation incorporates Patco's qualification.
[14] Patco's objection to this and other statements regarding the Modified eBanking Agreement on the ground of Tarte's lack of foundation as to personal knowledge, Plaintiff's Opposing SMF ¶¶ 28-31, is overruled. Tarte states
(continued on next page)

published as of May 2009. Defendant's SMF ¶ 29; Tarte Decl. ¶ 10.[15] The Modified eBanking Agreement could be accessed any time a customer logged into eBanking. Defendant's SMF ¶ 31; Tarte Decl. ¶ 11.

The Modified eBanking Agreement stated: "[I[f you use Ocean Bank eBanking . . . each party agrees to the terms and conditions stated in the Agreement." Defendant's SMF ¶ 33; Modified eBanking Agreement (Docket No. 68), Tab 1B to Appendix, § II.[16] The Modified eBanking Agreement explicitly described the option to receive email alerts. Defendant's SMF ¶ 34; Plaintiff's Opposing SMF ¶ 34. The Modified eBanking Agreement provided that use of Patco's eBanking password constituted Patco's signature authorization. Defendant's SMF ¶ 35; Modified eBanking Agreement § XVI.

The Modified eBanking Agreement also provided: "If you choose to receive ACH debit transactions on your commercial accounts, you assume all liability and responsibility to monitor those commercial accounts on a daily basis. In the event that you object to any ACH debit, you

---

that he has personal knowledge of the information set forth in his affidavit, Tarte Decl. at 1, and that, in his role as the Bank's Vice President of Information Security, he was familiar with the security procedures in place at Ocean Bank at all relevant times, including in May 2009, *id*. ¶¶ 5-6. This sets forth sufficient foundation for his personal knowledge of the circumstances of the creation and publication of the Modified eBanking Agreement, which touched, *inter alia*, on information security. To the extent that Patco protests that Ocean Bank fails to set forth the date of the publication of the Modified eBanking Agreement, Plaintiff's Opposing SMF ¶ 28, Ocean Bank remedies that omission in its reply statement of material facts, asserting that the Modified eBanking Agreement was continuously available on the Bank's website from August 21, 2008, through May 2009, when the alleged fraudulent withdrawals occurred, Defendant People['s] United Bank's Reply to Plaintiff's Statement of Additional Undisputed Material Facts ("Defendant's Reply SMF") (Docket No. 118) ¶ 1; Second Supplemental Declaration of Jeffrey R. Tarte in Support of Defendant People's United Bank's Reply Memorandum in Support of Its Motion for Summary Judgment ("Second Suppl. Tarte Decl.") (Docket No. 119), Tab 1 to Defendant People's United Bank's Master Second Supplemental Appendix in Support of Its Motions for Summary Judgment, To Strike Plaintiff's Jury Trial Demand, & *Daubert*/*Kumho* Motion To Exclude Expert Testimony of George F. Thomas ("Second Suppl. Appendix") (Docket No. 119), ¶ 4.

[15] I have modified the Bank's statement that the agreement was "in effect in May 2009[,]" sustaining Patco's objection, Plaintiff's Opposing SMF ¶ 29, that this states a legal conclusion. Patco further purports to deny this and other statements on the ground that it had no notice of the existence or terms of the Modified eBanking Agreement in May 2009 and, therefore, that agreement was not effective between the parties. *Id*. ¶¶ 29-33, 35-37, 40, 44-45, 47. However, the first portion of Patco's statement is in the nature of a qualification rather than a denial, and the second portion constitutes legal argument.

[16] I have modified the Bank's characterization of this section of the agreement, sustaining Patco's objection, Plaintiff's Opposing SMF ¶ 33, that the characterization is argumentative.

agree to notify us of your objection on the same day the debit occurs." Defendant's SMF ¶ 38; Plaintiff's Opposing SMF ¶ 38.[17] Patco received ACH debits on its account such as 401(k) contributions and state tax payments. *Id.* ¶ 39. A monitoring requirement is typically found in most financial services' end-user agreements involving money transfer capabilities. Defendant's SMF ¶ 43; Declaration of Peter A. Makohon in Support of Defendant People's United Bank's Motion for Summary Judgment ("Makohon Decl.") (Docket No. 69), Tab 2 to Appendix, ¶ 14.[18] Several provisions of the Modified eBanking Agreement state that a user should contact Ocean Bank immediately if it suspects unauthorized activity in its accounts. Defendant's SMF ¶ 45; Modified eBanking Agreement §§ X, XI, XIII.A. Section XIII.A of that agreement states that "[c]ontacting Ocean Bank right away will help you reduce possible losses." Defendant's SMF ¶ 46; Modified eBanking Agreement § XIII.A.

3. Credit Sweep Agreement

Patco entered the Sweep Agreement with Ocean Bank on September 5, 2003. Defendant's SMF ¶ 48; Plaintiff's Opposing SMF ¶ 48. Under the Sweep Agreement, funds from Patco's account were transferred by Ocean Bank into a separate investment account. *Id.* ¶ 49. The Sweep Agreement authorized Ocean Bank to "transfer to the Sweep Account from the Line of Credit an amount necessary to maintain: (i) any target balance in the Sweep Account established pursuant to paragraph 5 below, and (ii) a zero (0) balance in the designated operating

[17] My recitation incorporates Patco's qualification (mischaracterized as a denial).

[18] Patco's objection that Makohon fails to establish that he has personal knowledge of the end-user agreements of "most" financial services institutions, Plaintiff's Opposing SMF ¶ 43, is overruled. Makohon states that during his 14 years working in the financial services sector for Wachovia, one of the top five financial institutions in the United States, he became familiar with the security procedures of hundreds of financial services organizations of all sizes, and that he is familiar with the security measures used by various financial institutions during the relevant time period. Makohon Decl. ¶¶ 4-6. Patco denies the Bank's further statement that a customer is in a superior position to notice any suspicious transactions on its own account, asserting that the Bank is in as good or a superior position to notice any suspicious transactions on accounts. *Compare* Defendant's SMF ¶ 43 *with* Plaintiff's Opposing SMF ¶ 43.

accounts." *Id.* ¶ 50.[19] Patco was aware, and voluntarily accepted, that Ocean Bank would draw upon its line of credit if its checking account had insufficient funds. *Id.* ¶ 51. The Sweep Agreement was in effect in May 2009. *Id.* ¶ 52.

4. ACH Agreement

The ACH Agreement was in effect in May 2009. *Id.* ¶ 53. The ACH Agreement also governed the terms of Patco's use of electronic funds transfers through Ocean Bank via the ACH network. *Id.* ¶ 54. The ACH Agreement is signed by Mark Patterson, who authenticated his signature on the agreement at his deposition. *Id.* ¶ 55. McDowell also testified that his initials appear on the ACH Agreement. *Id.* ¶ 56.[20]

The ACH Agreement provided that Patco was responsible for electronic transfers "purport[ed] to have been transmitted or authorized" by Patco, even if a transfer was not authorized by Patco, "provided Bank acted in compliance with the security procedure referred to in Schedule A[.]" *Id.* ¶ 57.[21] The ACH Agreement expressly limited Ocean Bank's liability to gross negligence. Defendant's SMF ¶ 58; ACH Agreement § 12(a).[22] The ACH Agreement further limited liability by providing that "[i]n no event shall Bank be liable for any consequential, special, punitive or indirect loss or damage which Customer may incur or suffer in connection with this Agreement[.]" Defendant's SMF ¶ 59; ACH Agreement § 12(b).[23] The ACH Agreement provided: "This Agreement (including Schedule A attached hereto), together with the Account Agreement, is the complete and exclusive statement of the agreement between

[19] My recitation incorporates Patco's qualification.
[20] My recitation incorporates Patco's qualification.
[21] Patco qualifies this statement, asserting that the security procedures provided in Schedule A do not, by their express terms, apply to eBanking transactions. Plaintiff's Opposing SMF ¶ 57; ACH Agreement (Docket No. 68), Tab 1C to Appendix, § 13(a) & Schedule A thereto.
[22] Patco purports to deny this statement; however its argument that the cited language is ineffective to vary obligations imposed by law, Plaintiff's Opposing SMF ¶ 58, does not controvert the underlying fact.
[23] Patco purports to deny this statement; however its argument that the cited language is ineffective to vary obligations imposed by law, Plaintiff's Opposing SMF ¶ 59, does not controvert the underlying fact.

Bank and Customer with respect to the subject matter hereof[.]" Defendant's SMF ¶ 60; Plaintiff's Opposing SMF ¶ 60.[24]

5. ACH Limits

An ACH limit restricts a customer from exceeding a specified level of ACH activity in a single day. Plaintiff's SMF ¶ 97; Defendant's Opposing SMF ¶ 97. On behalf of the Bank, Kim S. Maxwell testified, "The limits are put in place after a discussion with the ACH originating customer to determine what their needs are and then those limits are established within the NetTeller system that restrict a customer from exceeding the limit that's been established in a single day." *Id.* ¶ 98; [Rule] 30(b)(6) Deposition of People's United Bank (Kim S. Maxwell) ("Maxwell Dep.") (Docket No. 96) at 187.[25]

Patco's ACH limit was initially set at $100,000. *Id.* ¶ 99. Prior to May 2009, it had been raised twice, first to $500,000, then to $750,000. *Id.* ¶ 100. The ACH limit was increased multiple times at Patco's request, to meet its stated need to make ACH transactions of increasing amounts. Defendant's SMF ¶ 191; Plaintiff's Opposing SMF ¶ 191.[26] Apart from any statement made in the ACH Agreement, the Bank made no effort to apprise Patco of possible risks of raising the ACH limit. Plaintiff's SMF ¶ 104; Defendant's Opposing SMF ¶ 104.[27] The ACH Agreement contained no statements apprising Patco of possible risks of raising the ACH limit or of maintaining a high ACH limit. *Id.* ¶ 105.

---

[24] My recitation incorporates Patco's qualification.
[25] My recitation incorporates Ocean Bank's qualification.
[26] Patco qualifies this statement, asserting that the Bank expressly recommended that Patco accomplish transfers from its account at Maine Bank & Trust to its account at Ocean Bank, necessitating the higher ACH limit. Plaintiff's Opposing SMF ¶ 191; McDowell Dep. at 92-93 (version filed at Docket No. 100-3).
[27] Ocean Bank qualifies this statement, asserting that, when Patco requested that its ACH limit be increased, Patco and the Bank did not discuss any risks. Defendant's Opposing SMF ¶ 104; [Rule] 30(b)(6) Deposition of People's United Bank (Matthew J. Stringer) and Matthew J. Stringer Individually ("Stringer Dep.") (Docket No. 96), Tab 4H to Suppl. Appendix, at 68-69.

C. Ocean Bank's Security Measures

1. Jack Henry Products

In 2004, Ocean Bank began using Jack Henry & Associates ("Jack Henry") to provide its core online banking platform, known as "NetTeller." Defendant's SMF ¶ 7; Plaintiff's Opposing SMF ¶ 7. Jack Henry has provided Ocean Bank with the NetTeller Internet banking platform since then. *Id*. ¶ 63. Jack Henry is a leading provider of computer systems and services to financial institutions nationwide, including a suite of online banking security and authentication solutions. *Id*. ¶ 64.[28]

Jack Henry provides the NetTeller product to approximately 1,300 of its 1,500 bank customers. *Id*. ¶ 65. NetTeller operates in an Application Service Provider ("ASP") environment, where the application is hosted at Jack Henry sites. *Id*. ¶ 66. The application uses a conduit to customer-specific accounting data that may reside either on a host at the financial institution or at a Jack Henry (or third party) data processing center. *Id*.

Jack Henry provides security for the systems it sells, including software patches, firewalls, anti-virus, and other security measures. *Id*. ¶ 67. Jack Henry's security systems are regularly audited by federal regulatory authorities for adherence to regulatory mandates. *Id*. Jack Henry's internal auditors and third parties perform additional reviews to ensure that the security systems in place are working as designed. *Id*.

[28] Patco qualifies this statement, characterizing the assertion that Jack Henry is a "leading provider" of such services as conclusory and argumentative. Plaintiff's Opposing SMF ¶ 64. The phrase at issue is more in the nature of a "fact" than an "argument." Patco's objection to the statement on the ground that Tarte lacks the foundation to make it, *id*., is overruled. Tarte served as Information Security Officer for Chittenden Bank from 1998 through 2008, a position in which he was responsible for information security program strategy. Tarte Decl. ¶ 5. In turn, Chittenden Bank worked with Jack Henry in 2006 to revamp Chittenden Bank's online authentication security. *Id*. ¶¶ 23-24.

2. 2005 FFIEC Guidance

In October 2005, the agencies of the Federal Financial Institutions Examination Council ("FFIEC") issued guidance titled "Authentication in an Internet Banking Environment" ("FFIEC Guidance" or "Guidance"). Plaintiff's SMF ¶ 22; Defendant's Opposing SMF ¶ 22.[29] The Guidance does not endorse any particular technology for compliance with the Guidance. Defendant's SMF ¶ 68; Plaintiff's Opposing SMF ¶ 68.[30] The Guidance states that "financial institutions should periodically . . . [a]djust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information[.]" *Id*. ¶ 69.[31] The Guidance also provides that "where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multi factor authentication, layered security, or other controls reasonably calculated to mitigate those risks." *Id*. ¶ 70.

The Guidance explains that existing authentication methodologies involve three basic "factors": (i) "[s]omething the user ***knows*** (e.g., password, PIN)"; (ii) [s]omething the user ***has*** (e.g., ATM card, smart card)"; and (iii) "[s]omething the user ***is*** (e.g., biometric characteristic, such as a fingerprint)." FFIEC Guidance at 3 (emphasis in original).[32] It states:

> Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a logon ID/password is single-factor

[29] My recitation incorporates Ocean Bank's qualification.

[30] Patco qualifies this statement, observing that the Guidance states that "[t]he agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties." Plaintiff's Opposing SMF ¶ 68; FFIEC Guidance (Docket No. 71), Tab 19 to Appendix, at 1.

[31] My recitation incorporates Patco's qualification.

[32] The parties neglected, in their statements of material facts, to set forth certain provisions of the FFIEC Guidance upon which they rely in their briefs. *See, e.g.*, Plaintiff's S/J Motion at 4. Because these provisions are important to understanding and/or resolution of the case, there is no material dispute concerning them, and the court in any event can take judicial notice of their existence, I have set them forth.

> authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication methodology may also include "out-of-band" controls for risk mitigation.

Id.[33] The Guidance also states:

> The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. . . . Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

Id. at 1-2. Financial institutions further are advised to "[a]djust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of [their] customer information, and internal or external threat to information" and to "implement appropriate risk mitigation strategies." *Id.* at 2.

In November 2005, Chittenden Bank stated in a Chittenden Audit Report that "[i]t is recognized in the industry that I[D]s and passwords, used alone (single factor), are not a secure method of system authentication. Passwords can be revealed relatively easily." Plaintiff's SMF ¶ 85; Defendant's Opposing SMF ¶ 85.

In 2006, following the publication of the FFIEC Guidance, Chittenden Bank, then an affiliate of Ocean Bank, conducted a comprehensive assessment to comply with the Guidance. Plaintiff's SMF ¶ 23; Defendant's Opposing SMF ¶ 23. Chittenden Bank identified Jack Henry's retail and commercial NetTeller product as involving high-risk transactions that required multifactor authentication. *Id.* Accordingly, the Bank broke out this system into a sub-project to

[33] "Out-of-band generally refers to additional steps or actions taken beyond the technology boundaries of a typical transaction." FFIEC Guidance at 3 n.5. "Callback (voice) verification, e-mail approval or notification, and cell-phone based challenge/response processes are some examples." *Id.*

implement stronger authentication. *Id*. Chittenden Bank put together a team of individuals to investigate how best to comply with the FFIEC Guidance. *Id*. The team worked with Jack Henry to identify the most appropriate solution to achieve compliance with the Guidance. *Id*.[34]

Following publication of the FFIEC Guidance, Jack Henry entered into a re-seller agreement with Cyota, Inc., an RSA Security Company ('RSA/Cyota") for a multifactor authentication system to integrate into its NetTeller product so that it could offer security solutions compliant with FFIEC Guidance. Defendant's SMF ¶ 71; Plaintiff's Opposing SMF ¶ 71.[35] RSA/Cyota is the industry leader for protecting online identities and digital assets. *Id*. ¶ 72. Security provided by RSA/Cyota is used by 90 percent of the Fortune 500 companies. *Id*.[36]

Jack Henry marketed its RSA/Cyota multifactor solution to its customers as "the most robust and effective solution available" as of 2006. *Id*. ¶ 73.[37] Jack Henry, through collaboration with RSA/Cyota, made two multifactor authentication products available to its customers to meet the FFIEC Guidance: the "Basic" package ("Basic Product") and the "Premium" package ("Premium Product"). *Id*. ¶ 74.

---

[34] My recitation incorporates Ocean Bank's qualification.

[35] Patco qualifies this and other statements, denying that the "Premium" authentication product used true multifactor authentication because it allowed a user's knowledge of a customer's challenge questions (something the user knows) to override the user's lack of anything the customer was or is. *See, e.g.*, Plaintiff's Opposing SMF ¶ 71. This critique is set forth in detail *infra*.

[36] Patco qualifies paragraph 72, characterizing the assertion that RSA/Cyota is "the industry leader" as conclusory and argumentative. Plaintiff's Opposing SMF ¶ 72. The phrase at issue is more in the nature of a "fact" than an "argument." Patco's objection that Debra L. Edwards, whose affidavit the Bank cites, lacks foundation to make the assertions contained in paragraph 72, *id*., is overruled. Edwards is Jack Henry's Senior Manager of Client Support, Internet Solutions. Declaration of Debra L. Edwards in Support of Defendant People's United Bank's Motion for Summary Judgment ("Edwards Decl.") (Docket No. 69), Tab 3 to Appendix, ¶ 5. Among Jack Henry's products are two authentication products developed in conjunction with RSA/Cyota. *Id*. ¶ 13.

[37] Patco qualifies this statement, denying that this advertising claim was true because, by 2007, authentication systems were widely available incorporating true multifactor authentication, tokens, and other means of generating one-time passwords, and true out-of-band authentication. Plaintiff's Opposing SMF ¶ 73. However, the citations provided do not support the proposition that these authentication systems were "widely available" by 2007.

With both the Basic and Premium products, when a customer logged onto online banking, it entered a company NetTeller ID and password and then an ID and password specific to each user. *Id.* ¶ 75. In addition to IDs and passwords, the Basic Product offered invisible device authentication and challenge/response questions. *Id.* ¶ 76. In addition to IDs and passwords, the Premium Product offered development of a customer profile, challenge/response questions, invisible device authentication, user-selected picture, IP Geo location, transaction monitoring, scoring engine for transactions, an eFraud Network subscription, and reporting. *Id.* ¶ 77.[38] The Premium Product cost $1,500 per banking division as a one-time installation fee and an additional 52 cents per enrolled Internet banking account. *Id.* ¶ 78. A one-time installation fee of $1,000 was charged for the Basic Product. *Id.*[39]

3. Implementation of New Authentication Product in 2007

a. Features of Jack Henry Premium Product

To comply with the Guidance, Ocean Bank selected the Jack Henry Premium Product at greater expense to the bank. *Id.* ¶ 80. The new system was implemented in January 2007. Plaintiff's SMF ¶ 25; Defendant's Opposing SMF ¶ 25. The system:

1. Passwords and IDs. Required each authorized Patco employee to use both a company ID and password and user-specific ID and password to access online banking. Defendant's SMF ¶ 82; Plaintiff's Opposing SMF ¶ 82;

2. Challenge Questions. Required users, during initial log-in, to select three challenge questions and responses. *Id.* ¶ 87. The challenge questions might be prompted for

[38] Patco qualifies this statement, asserting that Ocean Bank's system did not incorporate a user-selected picture and that, while the NetTeller system provided activity reports, Ocean Bank began reviewing them only after the fraud involving Patco occurred. Plaintiff's Opposing SMF ¶ 77; Maxwell Dep. (version filed at Docket No. 100-7) at 45, 127-30.

[39] Patco qualifies this statement, reckoning that because the Chittenden family of banks had approximately 30,000 customers in 2006 and 2007, the additional cost of the Premium Product to that entire family of banks was only approximately $16,100. Plaintiff's Opposing SMF ¶ 78; Maxwell Dep. (version filed at Docket No. 100-7) at 107.

various reasons. *Id.* For example, if the risk score associated with a particular transaction exceeded a certain amount, the challenge questions would be triggered. *Id.* ¶ 88. If the challenge question responses entered by the user did not match the ones originally provided, the customer would receive an error message. *Id.* ¶ 89. If the customer was unable to answer the challenge questions in three attempts, the customer was blocked from online banking and required to contact the bank. *Id.* Once a customer established answers to its challenge questions, the customer was not required to change its answers unless they were reset by the Bank. Plaintiff's SMF ¶ 52; Defendant's Opposing SMF ¶ 52. A Jack Henry document states that changing passwords periodically is "an essential piece of the online security puzzle." *Id.* ¶ 53;[40]

3. Risk Profiling. Entailed the building of a risk profile for each customer by RSA/Cyota from a number of different factors, such as the location from which a user logged in, when/how often a user logged in, and what a user did while on the system. *Id.* ¶ 83. The Premium Product noted the IP address that the customer typically used to log into online banking and added it to the customer profile. Defendant's SMF ¶ 114; Plaintiff's Opposing SMF ¶ 114. With the Basic product, there was protection at log-in only. *Id.* ¶ 115. RSA/Cyota's adaptive monitoring provided risk scoring to, among other things, every log-in attempt and transaction based on a multitude of data, including but not limited to IP, device cookie ID, Geo location, and transaction activity. Plaintiff's SMF ¶ 32; Defendant's Opposing SMF ¶ 32.[41] The Cyota unique profiling system was designed to take into account the circumstances of a customer known to the

[40] Ocean Bank qualifies this statement, asserting that this language should not be imputed to challenge questions.
[41] My recitation reflects Ocean Bank's qualification.

bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank. Defendant's SMF ¶ 157; Plaintiff's Opposing SMF ¶ 157.[42]

After the risk profile was complete, if a transaction showed up on that user's account that differed from its normal profile, the risk score associated with that transaction was elevated. *Id.* ¶ 84. Challenge questions were prompted any time the risk score for a transaction exceeded 750 on a scale of zero to 1,000. Plaintiff's SMF ¶ 34; Defendant's Opposing SMF ¶ 34.[43] RSA Security, Inc., the company that developed the risk-scoring application, considered transactions generating risk scores in excess of 750 to be high-risk transactions. *Id.* ¶ 35. The only result of a high-risk score was that a customer was prompted to answer his or her challenge questions. *Id.* ¶ 38;

4. Device Cookies. Placed a "device cookie" onto customers' computers to identify particular computers used to access online banking. Defendant's SMF ¶ 85; Plaintiff's Opposing SMF ¶ 85. The device cookie was used to help establish a secure communication session with the NetTeller environment and to establish the component risk score. *Id.* ¶ 86. If the cookie changed or was new, that impacted the risk score and potentially resulted in the user being challenged. *Id.*;

[42] Patco's objection to paragraph 157 on the basis that it fails to set forth each fact in a separately numbered paragraph as required by Local Rule 56(b), Plaintiff's Opposing SMF ¶ 157, is overruled. While paragraph 157 could and should have been shortened, Patco has not been rendered unable to respond properly and with clarity, as it asserts. *Id.* Patco alternatively qualifies the statement, asserting that, in May 2009, Ocean Bank had configured its system to ask challenge questions on every transaction regardless of the outcome of the Cyota profiling system, depriving the system of its behind-the-scenes functionality as a trigger for challenge questions, and Ocean Bank was not manually reviewing transactions that generated high risk scores in May 2009, depriving the Cyota profiling system of any practical utility. Plaintiff's Opposing SMF ¶ 157. This critique is set forth in detail *infra*.

[43] My recitation reflects Ocean Bank's qualification.

5. Dollar Amount Rule. Permitted financial institutions to set a dollar threshold amount above which a transaction would trigger the challenge questions even if the user ID, password, and device cookie were all valid (the "Dollar Amount Rule"). *Id.* ¶¶ 90, 94;[44]

6. Subscription to eFraud Network. Provided Ocean Bank with a subscription to the eFraud Network, which compared characteristics of the transaction (such as the IP address of the user seeking access to the Bank's system) with those of known instances of fraud. *Id.* ¶ 121; Plaintiff's SMF ¶ 36; Defendant's Opposing SMF ¶ 36. Subscription to the eFraud Network added a higher level of security beyond the individual customer authentication process. Defendant's SMF ¶ 122; Plaintiff's Opposing SMF ¶ 122. Any fraudulent activity, IP address, or other indicia identified and reported by a financial institution belonging to the eFraud Network was immediately blocked if someone attempted to access a customer's NetTeller account. *Id.* The individual would not even be prompted for challenge questions. *Id.*; and[45]

7. Reports to Financial Institutions. Provided reports to financial institutions *via* the Internet through the Cyota dashboard. *Id.* ¶ 123. With the Premium Product, financial institutions were provided all standard reports and allowed to create their own custom reports. *Id.*[46]

Not all the security procedures used by Ocean Bank are visible to customers. *Id.* ¶ 157. Security measures such as device ID, GeoIP, and cookies all happen in the background in order

[44] Financial institutions could set other transaction-based rules, such as rules based on transaction type (*e.g.*, ACH *versus* wire) or the location of an IP address in a foreign country, which would prompt the user to answer challenge questions if a particular type of transaction was made. Defendant's SMF ¶ 116; Plaintiff's Opposing SMF ¶ 116; Plaintiff's SMF ¶ 39; Defendant's Opposing SMF ¶ 39.

[45] Patco qualifies this statement, asserting that it contradicts the Bank's previous description of the eFraud Network as providing fraud scoring for all RSA customers. Plaintiff's Opposing SMF ¶ 122. I perceive no inherent conflict. The eFraud Network could serve both functions.

[46] Patco qualifies this statement, asserting that Ocean Bank did not review any reports showing suspicious or high-risk transactions prior to the fraud at Patco, and began reviewing such reports only in late 2009. Plaintiff's Opposing SMF ¶ 123; Maxwell Dep. (version filed at Docket No. 100-7) at 127-32.

to minimize disruption to customers' experience and the risk of criminals receiving and using the information. *Id.*

b. Parties' Understandings, Communications on Security Measures

Patco agreed to the use of security passcodes, which consisted of a customer ID and a customer password and a user ID and password for each authorized user of the customer. *Id.* ¶ 145. Patco used challenge questions both (1) in its initial selection of those questions and its input of the answers to those questions and (2) through its use, *i.e.*, when it logged on to online banking almost weekly over the course of years. *Id.* ¶ 146. Specifically, during initial log-in, the Ocean Bank system (through the Premium Product) would prompt every user to provide answers to three challenge questions, which would be used in the future to confirm that user's identity. *Id.*[47] Thus, Patco initially was required to select its preferences of three challenge questions from a drop-down list. *Id.* ¶ 147. Thereafter, it had to input the answers to those challenge questions. *Id.* These three questions, and the answers inputted by Patco, would become the challenge questions with which Patco was presented when it logged on. *Id.* Patco also answered those challenge questions when prompted to do so over the course of many years of logging into its online banking account on a weekly basis. *Id.*[48]

Prior to May 14, 2009, Patco did not communicate any wishes separate and apart from the security procedures included in the agreements governing eBanking and the eBanking for Business User Guide. Defendant's SMF ¶ 148; Tarte Decl. ¶ 40. Patco never expressed its dissatisfaction with these security procedures to Ocean Bank personnel. Defendant's SMF

[47] Patco's objection to paragraph 146 on the grounds that it is argumentative, conclusory, and not provided by the record citation provided, Plaintiff's Opposing SMF ¶ 146, is sustained in part, to the extent that I have edited the statement, and otherwise overruled.

[48] Patco's objections to paragraph 147 on the grounds that it is argumentative, conclusory, and not supported by the record citation provided, and that Tarte lacks foundation for his assertion that Patco answered challenge questions over the course of many years, Plaintiff's Opposing SMF ¶ 147, are sustained in part, to the extent that I have edited the statement, and otherwise overruled.

¶ 149; Tarte Decl. ¶ 40. Likewise, prior to May 14, 2009, Patco had not sought any additional protections or expressed dissatisfaction with the eBanking security procedures offered. Defendant's SMF ¶ 150; [Rule] 30(b)(6) Deposition of Patco Construction Company, Inc. (Thomas P. McDowell) and Thomas P. McDowell Individually ("McDowell Dep.") (Docket No. 70), Tab 5 to Appendix, at 226.[49]

McDowell could not recall the specifics of discussions with anyone at Ocean Bank about the eBanking agreement. Defendant's SMF ¶ 151; Plaintiff's Opposing SMF ¶ 151.[50] Patco continued to use eBanking on at least a weekly basis, using the security procedures in place. *Id.* ¶ 152.[51] Patco also agreed that it was responsible for all of the transfers and bill payments that it authorized, including any transactions authorized by third parties that Patco permitted to use its password. *Id.* ¶ 153. Patco further agreed that use of a user's password constituted authentication of all transactions performed by the user or on the user's behalf. *Id.* ¶ 154.

c. Ocean Bank's Configuration of Dollar Amount Rule

The Dollar Amount Rule was among configurations known as "rules" that Jack Henry allowed financial institutions to modify. *Id.* ¶ 94. For those configurations that Jack Henry

[49] Patco purports to deny or qualify paragraphs 148 through 150 on the ground that Patco expressly requested that the Bank send email alerts to Patco on every ACH transaction it initiated, and the Bank agreed, but then failed, to do so. Plaintiff's Opposing SMF ¶¶ 148-50; *see also* Plaintiff's SMF ¶¶ 111-13. Nonetheless, as Ocean Bank points out, Defendant's Opposing SMF ¶¶ 111-13, the request on which Patco relies, emailed by McDowell to the Bank on March 23, 2004, is taken out of context. McDowell's request predated the availability of email alerts, which were first made available to the Bank's customers on December 1, 2006, and McDowell testified that he was not aware that email alerts were available. *Id.* ¶ 111; Suppl. Tarte Decl. ¶ 14; McDowell Dep. at 225. McDowell's request evidently pertained to Patco's practice of emailing Ocean Bank to request transfers from accounts that were not set up for eBanking, with McDowell seeking confirmation that transfers requested by email had been completed. Defendant's Opposing SMF ¶¶ 111-13; Deposition of Diana Pierce ("Pierce Dep.") (Docket No. 71), Tab 12 to Appendix, at 42; Exh. 1 to Declaration of Thomas P. McDowell ("McDowell Decl.") (Docket No. 74-4); Tabs 4I-4K (Docket No. 96) to Suppl. Appendix.

[50] My recitation incorporates Patco's qualification.

[51] Patco qualifies this statement, asserting that, as the Bank itself elsewhere notes, certain security procedures were not visible to customers, and the Bank should not have expected Patco to be in a position to evaluate and understand its online authentication security procedures, which were not expressly made clear. Plaintiff's Opposing SMF ¶ 152; Supplemental Declaration of Sari Stern Greene ("Suppl. Greene Decl.") (Docket No. 99-1) ¶ 37.

allowed its customers to change, Jack Henry had determined that any configuration that the customer chose would result in the effective operation of the multifactor authentication product. *Id.* ¶ 95.[52] Jack Henry determined that a customer could set the Dollar Amount Rule at any particular dollar amount threshold, and its product would operate effectively. *Id.* ¶ 96. Jack Henry allowed modification of particular configurations in certain circumstances, such as the Dollar Amount Rule, because such settings were purely matters of business discretion rather than security (*i.e.*, the rules could be set by a bank at points reasonable for the particular bank, dependent on the bank's customer base, issues of customer convenience, usability, and so on). Defendant's SMF ¶ 97; Edwards Decl. ¶ 26.[53]

Jack Henry's default setting for the Dollar Amount Rule was $1,000. Defendant People['s] United Bank's Additional Statement of Material Facts ("Defendant's Additional SMF"), commencing on page 48 of Defendant's Opposing SMF, ¶ 17; Plaintiff's Reply Statement of Material Facts ("Plaintiff's Reply SMF") (Docket No. 110) ¶ 17. If the customer did not change the default setting, the Dollar Amount Rule would remain set at $1,000. *Id.* ¶ 18. Jack Henry believed that it would be reasonable for bank customers either to leave the Dollar Amount Rule set at the default of $1,000 or to modify it as their business needs changed or as various events, such as low-dollar frauds, occurred. *Id.* ¶ 19. The system permitted banks to set the Dollar Amount Rule at any dollar amount, from $1 up. *Id.*

The $1,000 default Dollar Amount Rule set by Jack Henry was not rolled out to Jack Henry's Premium customers, including Ocean Bank, until August 2007, and, therefore, the

[52] Patco qualifies this and other statements, *see, e.g.*, Plaintiff's Opposing SMF ¶ 95, asserting that the setting of the Dollar Amount Rule played an integral role in the effectiveness of Jack Henry's system. This point is set forth in detail *infra*.

[53] By contrast, Jack Henry did not allow financial institutions to modify challenge question collection settings that required users to provide answers to three challenge questions and triggered the blocking of the online banking account if challenge questions were answered incorrectly three times. Defendant's SMF ¶¶ 92-93; Plaintiff's Opposing SMF ¶¶ 92-93.

default Dollar Amount Rule was not implemented in Ocean Bank's Premium Product until then. *Id.* ¶ 20.[54] In August 2007, Ocean Bank set the Dollar Amount Rule to $100,000. Defendant's SMF ¶ 101; Plaintiff's Opposing SMF ¶ 101. The Dollar Amount Rule was set at $100,000 to ensure that customers were not inconvenienced by frequent prompts for challenge questions. *Id.* Ocean Bank also considered current information regarding ACH fraud known in the banking industry at that time in setting the Dollar Amount Rule. *Id.*[55]

On June 6, 2008, Ocean Bank intentionally lowered the Dollar Amount Rule from $100,000 to $1. *Id.* ¶ 103. Neither Jack Henry, RSA Security, nor any other outside security consultant or professional recommended that the Bank set the threshold for challenge questions at any particular dollar amount. Plaintiff's SMF ¶ 46; Maxwell Dep. (version filed at Docket No. 100-7) at 144-45.[56] After the Bank lowered the threshold to $1, Patco was prompted to answer challenge questions every time it initiated an ACH transaction, for instance its weekly ACH payroll transactions. Plaintiff's SMF ¶ 45; Pierce Dep. at 87-88.[57] In May 2009, the Dollar Amount Rule threshold was set at $1. Plaintiff's SMF ¶ 48; Defendant's Opposing SMF ¶ 48. In February 2010, the Bank raised the dollar amount threshold from $1 to $6,000. *Id.* ¶ 49.[58]

---

[54] Patco qualifies paragraphs 17 through 20, asserting that (i) Jack Henry did not make any specific dollar threshold recommendations, (ii) the Bank understood that it had the responsibility to decide the amount at which the Dollar Amount Rule should be set, and (iii) it would not have been reasonable from a security perspective for Jack Henry to implement a "one-size-fits-all" Dollar Amount Rule threshold for all of its NetTeller customers. Plaintiff's Reply SMF ¶¶ 17-20; Maxwell Dep. (version filed at Docket No. 100-7) at 144-45; Second Supplemental Declaration of Sari Stern Greene ("Second Suppl. Greene Decl.") (Docket No. 109-1) ¶ 3.

[55] Patco qualifies this statement, asserting that Maxwell, who was designated by Ocean Bank to testify on the configuration by the bank of its security procedures, testified that the $100,000 threshold was set "where we believed there was a balance between customer experiences, as well as the fraud that was occurring in the industry at that time." Plaintiff's Opposing SMF ¶ 101; Continued Deposition of Kimberly Maxwell ("Continued Maxwell Dep.") (Docket No. 100-8) at 24.

[56] Ocean Bank purports to deny this statement but fails to controvert it. Defendant's Opposing SMF ¶ 46.

[57] Ocean Bank purports to deny this statement but fails to controvert it. Defendant's Opposing SMF ¶ 45.

[58] Ocean Bank qualifies this statement, asserting that, as the threat landscape evolved and cybercriminals became more sophisticated, it reassessed and changed the Dollar Amount Rule threshold from time to time and purposely changed the challenge question amount triggers from time to time to thwart fraudsters' software that was designed to identify the online system's default dollar amount threshold. Defendant's Opposing SMF ¶ 49; Tarte Decl. ¶ 32. It *(continued on next page)*

Ocean Bank states that it lowered the Dollar Amount Rule threshold to $1 as a means to enhance security for its customers after the occurrence of ACH frauds at Ocean Bank that targeted low-dollar amount ACH transactions, Defendant's SMF ¶ 104; Tarte Decl. ¶ 32, with fraudsters having begun making fraudulent withdrawals at very low amounts in an attempt to "fly under the radar," Defendant's SMF ¶ 105; Continued Maxwell Dep. at 34, 41; Tarte Decl. ¶ 32; Makohon Decl. ¶ 23. Patco disputes this, noting, *inter alia*, that Maxwell testified that the decision to lower the threshold was not based on specific dollar amounts. Plaintiff's Opposing SMF ¶¶ 104-05; Maxwell Dep. (version filed at Docket No. 100-7) at 146. With respect to the two incidents of fraud on the Bank's system prior to May 2009, individuals with access to the customer's company IDs, passwords, user IDs, and user passwords were prompted for challenge questions. Plaintiff's Local Rule 56(c) Statement of Additional Material Facts ("Plaintiff's Additional SMF"), commencing on page 96 of Plaintiff's Opposing SMF, ¶ 3; Defendant's Reply SMF ¶ 3.[59] With respect to these prior instances of fraud, the Bank believed that the fraud was likely to have been perpetrated by means of keylogging malware or as a result of internal fraud. Plaintiff's SMF ¶ 96; [Rule] 30(b)(6) Deposition of People's United Bank (Jeffrey R. Tarte) and Jeffrey R. Tarte Individually ("Tarte Dep.") (Docket No. 75-9) at 32-34.[60]

Ocean Bank further states that the lowering of the Dollar Amount Rule threshold did in fact increase the security of online banking for customers because it added an additional layer of security every time a customer initiated an ACH transaction. Defendant's SMF ¶ 106; Tarte

states that, specifically, malware code was designed by cybercriminals to target certain perceived thresholds, and by varying its Dollar Amount Rule thresholds, Ocean Bank endeavored to interfere with criminals' malware code. *Id*.

[59] My recitation incorporates Ocean Bank's qualification.

[60] Ocean Bank purports to deny this statement, Defendant's Opposing SMF ¶ 96, but its denial is in the nature of a qualification: that Tarte testified that the Bank believed that malware and internal fraud were two possible options, although there could have been other causes, Tarte Dep. at 32-33.

Decl. ¶ 32; Makohon Decl. ¶ 23.[61] There was no fraud in the approximately one-year period following the institution of the $1 limit until the alleged fraudulent withdrawals from Patco's account. Defendant's SMF ¶ 113; Plaintiff's Opposing SMF ¶ 113.[62]

Patco disputes this point as well, stating that, while Jack Henry may have believed that customers could change rules settings, such as the Dollar Amount Rule, without affecting security, Jack Henry was wrong. *See* Plaintiff's Opposing SMF ¶¶ 95-96. Patco states that rules such as the Dollar Amount Rule played an integral role in the effectiveness of the security procedures on Jack Henry's system, pointing to a passage from RSA's Rules Management User Guide that provides:

> **Warning:** Decision rules must be edited **carefully**, slowly, with great caution. These rules are very powerful, directly affecting the customer experience of genuine users as well as playing a major role in fraud prevention.

Plaintiff's Opposing SMF ¶¶ 95-97; Exh. 55 to Continued Maxwell Dep. at PUB_0016391 (boldface in original). Patco also relies on testimony of its expert, Sari Greene, that setting challenge questions to be asked on every transaction greatly increases the risk that a fraudster equipped with a keylogger will be able to compromise the answers to a customer's challenge questions because it increases the frequency with which such information is entered through a

[61] Patco objects to paragraphs 104 and 105 on the basis of the asserted lack of personal knowledge of the declarants on whom the Bank relies, Tarte, Maxwell, and Makohon, none having provided any explanation as to the number or specific amounts of purported low-dollar transactions that prompted the change in the rule. Plaintiff's Opposing SMF ¶¶ 104-05. The objection is overruled. The lack of detail does not necessarily signal a lack of personal knowledge of the fact that low-dollar frauds prompted the rule change.

[62] Patco qualifies this statement, asserting that there also had been no ACH fraud during the period between Ocean Bank's implementation of its new authentication system in January 2007 and the frauds on Ocean Bank's system in May and June 2008, during which time Ocean Bank had either no dollar amount threshold or a $100,000 threshold. Plaintiff's Opposing SMF ¶ 113; Tarte Dep. at 29-30; Continued Maxwell Dep. at 18-19, 23. Patco adds that a fourth instance of fraud occurred in January 2010, at which time the Bank still had in place its $1 limit, after which it raised the limit to $6,000. Plaintiff's Opposing SMF ¶ 113; Tarte Dep. at 29-30; Continued Maxwell Dep. at 42-43.

user's keyboard. Plaintiff's Opposing SMF ¶ 96; Declaration of Sari Stern Greene ("Greene Decl.") (Docket No. 74-1) ¶¶ 19-26, 32.[63]

Ocean Bank denies that the lowering of the Dollar Rule Amount threshold to $1 meant that users were prompted to answer challenge questions every time they initiated an ACH or wire transfer transaction on their accounts, observing that the eFraud Network would immediately block a transaction without asking challenge questions if the transaction involved fraudulent activity, an IP address, or other indicia reported to the eFraud Network. Defendant's Opposing SMF ¶ 44; Edwards Decl. ¶ 19.

d. Whether Ocean Bank Had "True" Multifactor Authentication

Ocean Bank describes the Premium Product as offering multifactor authentication based on its employment of three relevant factors: "something the user knows," "something the user has," and "something the user is." Defendant's SMF ¶¶ 160-63. There is no dispute that Ocean Bank's security procedures employed "something the user knows": IDs and passwords and answers to challenge questions. Defendant's SMF ¶ 160; Plaintiff's Opposing SMF ¶ 160. Ocean Bank asserts, and Patco denies, that its security procedures also employed "something the user has": device identification information specific to the client's personal computer and its use of the Bank's application, and "something the user is": taking into account user behavior. *Compare* Defendant's SMF ¶¶ 161-63; Edwards Decl. ¶ 24; Makohon Decl. ¶ 17; FFIEC Guidance at 7 *with* Plaintiff's Opposing SMF ¶¶ 161-63; Greene Decl. ¶¶ 17-18; Suppl. Greene Decl. ¶¶ 12-13.

[63] A "keylogger" is a form of computer malware, or malicious code, capable of infecting a user's system, secretly monitoring the user's Internet activity, recognizing when the user has browsed to the website of a financial institution, and recording the user's key strokes on that website. Greene Decl. ¶ 20. In this way, the keylogger is able to capture a user's authentication credentials, which the keylogger then transmits to a cyber thief. *Id.*

Patco states that because, as of May 2009, the Bank had configured its security procedures such that challenge questions were triggered on every transaction regardless of the outcome of the device identification system, that system did not trigger any additional security and, accordingly, the Bank's security procedures did not employ "something the user has." Plaintiff's Opposing SMF ¶ 161; Suppl. Greene Decl. ¶¶ 12-13. Patco asserts that the third authentication factor, "something the user is," refers to physical (biometric) characteristics, not behavior patterns. Plaintiff's Opposing SMF ¶ 163; FFIEC Guidance at 7, 9-11. In any event, Patco states, because the Bank configured its procedures to trigger challenge questions on every transaction, the behavioral profiling system did not trigger any additional security. Plaintiff's Opposing SMF ¶ 163; Suppl. Greene Decl. ¶¶ 12-13.

Ocean Bank responds that the fact that the Jack Henry Premium Product may respond to various factors in a particular way, for example, by asking the user for "something the user knows," does not negate the existence of the other factors. Defendant's Additional SMF ¶ 22; Supplemental Declaration of Debra L. Edwards in Support of Defendant People's United Bank's Opposition to Patco Construction Company, Inc.'s Motion for Summary Judgment ("Suppl. Edwards Decl.") (Docket No. 96), Tab 3 to Suppl. Appendix. It states that the FFIEC Guidance explains that a multifactor system must include at least two of the three basic factors, but says nothing about how banks must respond when one of these factors detects an anomaly (*e.g.*, the system recognizes an unusual device ID). *Id.*

In addition to being multifactor, Jack Henry's Premium Product also contains "layered security" and has "other controls," both of which (in Ocean Bank's view) also satisfy the FFIEC Guidance. Defendant's Additional SMF ¶ 23; Suppl. Edwards Decl. ¶ 6; Supplemental Declaration of Peter A. Makohon in Support of Defendant People's United Bank's Opposition to

Patco Construction Company, Inc.'s Motion for Summary Judgment ("Suppl. Makohon Decl.") (Docket No. 96), Tab 2 to Suppl. Appendix, ¶ 17.[64]

Ocean Bank's security procedures are multilayered because they employ challenge questions as well as user IDs/passwords. Defendant's Additional SMF ¶ 24; Plaintiff's Reply SMF ¶ 24. The "other controls" that the Bank employed (*i.e.*, controls in addition to ID/passwords and challenge questions) that, in its view, satisfied the FFIEC Guidance included SSL encryption, invisible device authentication (device cookies), IP Geo location, transaction monitoring, scoring engine for transactions, customer profile, an eFraud Network subscription, reporting, commercial third-party anti-phishing services, posting of fraud alerts on the eBanking website, and email alerting. Defendant's Additional SMF ¶ 25; Suppl. Makohon Decl. ¶ 17.[65]

4. Security Measures Implemented in Addition to the Premium Product

a. Email Alerts

Ocean Bank first offered email alerts to its eBanking customers beginning on December 1, 2006. Defendant's Additional SMF ¶ 21; Plaintiff's Reply SMF ¶ 21. At that time, the Bank began actively promoting the alerts to customers. *Id.* Email alerts were available on the NetTeller website. Defendant's SMF ¶ 126; Plaintiff's Opposing SMF ¶ 126.[66] The cover letter enclosing a copy of the Original eBanking Agreement stated that if Patco had any questions, it should check the user guide online or screen-by-screen icons. *Id.* ¶ 127.[67] The eBanking for

[64] Patco purports to deny this statement, Plaintiff's Reply SMF ¶ 23, but the cited portions of the Greene declarations on which it relies do not controvert that the Premium Product was layered or had other controls, although Greene does challenge the effectiveness of the Premium Product as configured by the Bank, Greene Decl. ¶¶ 17-18, 32; Suppl. Greene Decl. ¶¶ 7-13.

[65] Patco's denial is in the nature of a qualification: It denies that the other controls employed by the Bank satisfied the FFIEC Guidance, were commercially reasonable, or constituted multifactor authentication. Plaintiff's Reply SMF ¶ 25; Greene Decl. ¶¶ 17-18, 32; Suppl. Greene Decl. ¶¶ 7-13.

[66] Patco qualifies these statements, asserting that it never saw anything from the Bank indicating that email alerts were available. Plaintiff's Opposing SMF ¶ 126; McDowell Dep. at 176-78; Plaintiff's Reply SMF ¶ 21.

[67] My recitation incorporates Patco's qualification.

Business User Guide, available on Ocean Bank's eBanking website, also provides instructions on how to set up email alerts. *Id*. ¶ 128.[68] A user need only click on a tab visible on the eBanking web page in order to set up the alerts. *Id*. ¶ 129.[69]

Diana Pierce, the Patco employee with primary responsibility for eBanking, admitted navigating to the Preferences tab on at least one occasion, although she did not recall what then happened. *Id*. ¶ 130.[70] McDowell admitted that he never went online and looked at the user guide. *Id*. ¶ 131. Patco did not set up email alerts through the eBanking system. Defendant's SMF ¶ 133; Tarte Decl. ¶ 35.[71]

b. Anti-Phishing Controls

In 2007, Ocean Bank increased the controls it had on anti-phishing above and beyond the Jack Henry security procedures, which also used anti-phishing starting in or about 2007, and beyond those used by similarly situated banks. Defendant's SMF ¶ 135; Plaintiff's Opposing SMF ¶ 135.[72] The specific product that Ocean Bank used to counter phishing attacks was called "counterphish." *Id*. In 2009, before the allegedly fraudulent withdrawals, Ocean Bank subscribed to another anti-phishing service. *Id*. ¶ 136. At the time of the alleged theft, Ocean

[68] Patco qualifies this statement, asserting that it did not see the eBanking for Business User Guide on the Bank's website. Plaintiff's Opposing SMF ¶ 128; McDowell Dep. at 176-78.

[69] Patco purports to deny this statement, but its denial is in the nature of a qualification: It asserts that setting up alerts on the eBanking system required a user to first click on the "Preferences" tab, which was visible from the eBanking web page, and then click a second tab labeled "Alerts," visible only from the Preferences page. Plaintiff's Opposing SMF ¶ 129; eBanking for Business User Guide (Docket No. 68), Tab 1E to Appendix, at PUB_0018085. The user then would have to follow a specific set of procedures to activate individual alerts. *Id*.

[70] My recitation incorporates Patco's qualification (mislabeled as a denial).

[71] Patco purports to deny this, asserting that it specifically requested that the Bank provide such alerts, and the Bank agreed but failed to do so. Plaintiff's Opposing SMF ¶ 133. However, as noted above, the Bank demonstrates that the request in question, made by McDowell on March 23, 2004, was not for alerts tied to eBanking.

[72] So-called "man in the middle" or "phishing" attacks generally function by redirecting the user to a spoof website that is designed to mimic a bank's site, which prompts customers to input their confidential log-in information. Greene Decl. ¶ 26.

Bank had at least two independent anti-phishing services available and one from Jack Henry. *Id.*[73]

c. Secure Socket Layer

In addition to the Premium Product, Ocean Bank used secure socket layer ("SSL") encryption on its main banking page before customer log-in to online banking. *Id.* ¶ 137. SSL comprises crypotographic protocols that provide security for communications over networks such as the Internet, and appear in a website's URL as "https//" instead of "http//." *Id.* ¶ 138. In particular, Ocean Bank used a Secure Site Pro digital certificate from VeriSign that forces a browser to use the stronger 128-bit encryption as the minimum strength to encrypt data transmitted over the Internet. *Id.* This added security above and beyond the Secure Site solution and was a more expensive product. *Id.*[74]

d. Phishing and Fraud Alerts

Since 2008, Ocean Bank has posted phishing and fraud alert notices to its customers on its main log-in screen, as well as on the main website, www.ocean.com. *Id.* ¶ 139. Such notices would "pop up" on the screen immediately upon the customer's log-in to the eBanking website. *Id.* ¶ 140. On June 30, 2008, Ocean Bank posted a notice on its website stating: "Please be advised that Ocean Bank has seen evidence of ACH fraud in your area. Our security features remain strong and in place. However, we need your help to combat fraud. Taking the following measures will help to ensure your security. Secure all eBanking IDs and Passwords. Monitor all account daily activity and notify us immediately if you notice anything which appears unusual or

[73] Patco purports to qualify paragraphs 135 and 136, as well as other statements by Ocean Bank, on the ground that the security measures discussed are not "security procedures" as defined in Article 4A of the Uniform Commercial Code ("UCC"). *See, e.g.*, Plaintiff's Opposing SMF ¶¶ 135-36. This is not a factual qualification but, rather, a legal argument.

[74] Patco qualifies this statement, asserting, in relevant part, that SSL encryption is commonly used, relatively inexpensive, and not intended to protect against keylogging malware. Plaintiff's Opposing SMF ¶ 138; Suppl. Greene Decl. ¶ 17.

out of the ordinary patterns of your business. Call 1-800-206-3790 to report your concerns." *Id.* ¶ 141.[75]

All of the above security procedures were in effect in May 2009, at the time of the alleged fraudulent withdrawals. *Id.* ¶ 143.[76]

5. Security Measures Not Implemented

a. Out-of-Band Option

In 2006 and 2007, when Ocean Bank initially implemented its authentication system in response to the FFIEC Guidance, the Bank was offered by Jack Henry, but declined, a version of the NetTeller system that included an out-of-band authentication option. Plaintiff's SMF ¶ 118; Defendant's Opposing SMF ¶ 118.[77]

b. Monitoring of Risk-Scoring Reports

In May 2009, Bank personnel did not monitor the risk-scoring reports received as part of the Premium Product package, nor did the Bank conduct any other regular review of transactions

[75] Patco qualifies paragraphs 139 through 141, asserting that website postings, particularly pop-up notices, are an insufficient means of informing customers of important security procedure updates because many browsers and anti-malware programs are configured to block pop-up messages. Plaintiff's Opposing SMF ¶¶ 139-41; Suppl. Greene Decl. ¶ 32. It also states that Ocean Bank has no evidence that anyone from Patco saw the described notices. Plaintiff's Opposing SMF ¶ 141.

[76] Patco qualifies this statement, Plaintiff's Opposing SMF ¶ 143, asserting, in relevant part, that, in May 2009, (i) the Bank was not actively reviewing any reports produced by the NetTeller system, Maxwell Dep. (version filed at Docket No. 100-7) at 131-32, and (ii) the transaction-monitoring and risk-scoring engines were not used by the Bank in any meaningful way because they were used to prompt challenge questions, and the Bank had lowered the dollar amount threshold to prompt challenge questions to $1, Continued Maxwell Dep. at 41; Pierce Dep. at 87-88.

[77] Ocean Bank qualifies this statement, asserting that it did not opt for Jack Henry's out-of-band option because it allowed the end-user to choose, when prompted with challenge questions, whether to answer the questions or have the system call the user with a new passcode for the user to input into the computer. Defendant's Opposing SMF ¶ 118; Edwards Decl. ¶ 14. Ocean Bank states that a fraudster who had already obtained answers to the challenge questions through malware could simply choose to answer the challenge questions. *Id.* Ocean Bank asserts that it had determined, as well, that Jack Henry's configuration allowed customers to input and change their own phone numbers. Defendant's Opposing SMF ¶ 118; Tarte Decl. ¶ 27. Accordingly, a fraudster who obtained a customer's ID and password could change the customer's phone number so that the system would call the fraudster rather than the true customer. *Id.* For these reasons, Ocean Bank explains, it determined that Jack Henry's out-of-band feature provided little to no benefit in an overall security framework. *Id.*; *see also* Defendant's SMF ¶ 81; Tarte Decl. ¶ 27. Patco asserts that, according to the RSA Customer Service Guide, financial institutions could choose whether to use out-of-band or challenge-response only, or a combination of the two, in which case the financial institution could specify which technology would be used first. Plaintiff's Opposing SMF ¶ 81; Customer Service User Guide (Docket No. 74-1), Exh. 10 to Greene Decl., at PUB_0015796.

that generated high risk scores. Plaintiff's SMF ¶ 37; Defendant's Opposing SMF ¶ 37.[78] In May 2009, the Bank had the capability to conduct manual reviews of high-risk transactions. *Id.* ¶ 86. Ocean Bank did not conduct such reviews in May 2009. *Id.* ¶ 87. The Bank began conducting manual reviews of high-risk transactions in late 2009. *Id.* ¶ 88. In May 2009, the Bank had the capability to conduct manual review of high-risk transactions through its transaction-profiling and risk-scoring system, but did not do so. *Id.* ¶ 109. The Bank had the ability to call a customer if it detected fraudulent activity. *Id.* ¶ 110.

In the case of uncharacteristic transactions, the Bank now calls the customer to inquire if the customer did indeed initiate the transaction. Plaintiff's SMF ¶ 89; Maxwell Dep. (version filed at Docket No. 100-7) at 129.[79] The Bank added manual reviews as a result of increased fraud in the ACH network. Plaintiff's SMF ¶ 90; Defendant's Opposing SMF ¶ 90. The Bank became aware of this increased fraud in the ACH network throughout 2009. *Id.* ¶ 91.[80] By May 2009, Ocean Bank was aware of two, possibly three, prior incidents of ACH fraud on its eBanking system that had occurred in May and June 2008. *Id.* ¶¶ 93-94.

[78] Ocean Bank qualifies this and other statements made by Patco pertaining to manual review, asserting that (i) the Jack Henry Premium Product system that it employed did not require manual review, (ii) in May 2009, the Premium Product system generated reports that included hundreds of events each day, including a great many events other than ACH transactions, such as log-ins or other activities that did not involve the transfer of money, and numerous "false positives," and (iii) over time, it became more feasible to manually review risk-scoring reports. Defendant's Opposing SMF ¶ 37; Suppl. Tarte Decl. ¶ 13. Ocean Bank adds that Patco itself logged into its eBanking account six times during the week of the alleged fraudulent withdrawals but failed to notice and report the suspicious activity. Defendant's Opposing SMF ¶ 37; Tarte Decl. ¶ 46.

[79] Ocean Bank purports to deny this statement, but its denial is in the nature of a qualification: that Maxwell testified that, when a risk score is above a certain amount, the Bank first compares the transaction against the customer's transaction history to determine if it is typical for that customer to be originating that amount that day and then examines the IP address from which the transactions are made to determine if it is an atypical IP address for the customer, only calling the customer if it determines that the transaction is not typical. Defendant's Opposing SMF ¶ 89; Maxwell Dep. (version filed at Docket No. 100-7) at 129-30.

[80] Ocean Bank qualifies this statement, asserting that it became aware in 2008 that fraudsters had begun making fraudulent withdrawals in very low amounts, after which it implemented "pop-up" notices to its customers alerting them of the need to monitor their accounts on a daily basis and lowered the amount of its Dollar Amount Rule to $1. Defendant's Opposing SMF ¶ 91; Continued Maxwell Dep. at 34, 41; Tarte Decl. ¶¶ 32, 37.

c. Tokens

A token-based solution was not available from Jack Henry when Ocean Bank implemented the Premium Product in 2007. Defendant's SMF ¶ 165; Plaintiff's Opposing SMF ¶ 165.[81] Jack Henry began testing tokens with just a few of its customers in January 2009. *Id.* ¶ 166. In May 2009, less than 2 percent of Jack Henry NetTeller customers were using tokens. *Id.* ¶ 167. Today, only 25 percent of Jack Henry's customers offer tokens to some or all of their customers. *Id.* ¶ 168.[82]

In May 2009, People's United Bank used tokens for its ACH and wire origination customers. Plaintiff's SMF ¶ 106; Defendant's Opposing SMF ¶ 106.[83] In May 2009, Wachovia used tokens for its commercial accounts. *Id.* ¶ 107.[84] Ocean Bank recently began offering tokens to its customers that originate ACH transfers. *Id.* ¶ 117.

d. User-Selected Picture

Ocean Bank's security procedures did not include the user-selected picture function that was available through Jack Henry's Premium option. Plaintiff's Additional SMF ¶ 2; Defendant's Reply SMF ¶ 2.[85]

---

[81] "Tokens are physical devices (*something the person has*) and may be part of a multifactor authentication scheme." FFIEC Guidance at 8 (emphasis in original). The FFIEC Guidance provides examples of three types of tokens: a USB token device, a smart card, and a password-generating token. *Id.* Patco qualifies paragraph 165, asserting that tokens were readily available to financial institutions at that time through other sources. Plaintiff's Opposing SMF ¶ 165; Suppl. Greene Decl. ¶ 21.

[82] Patco qualifies this statement, asserting that it does not account for customers that have requested token technology and are waiting for it to be implemented. Plaintiff's Opposing SMF ¶ 168; Suppl. Greene Decl. ¶ 22.

[83] Ocean Bank qualifies this statement, asserting that People's United Bank, unlike Ocean Bank, used an in-house online banking system and was not dependent on third-party banking platform providers. Defendant's Opposing SMF ¶ 106; Suppl. Tarte Decl. ¶ 12.

[84] The Bank's objection on the ground that this fact is irrelevant and immaterial, given that the Bank has no way of verifying whether every Wachovia customer used tokens, that Wachovia, a national bank, is not similarly situated to Ocean Bank, and that tokens can be compromised and deliver a false sense of security, Plaintiff's Opposing SMF ¶ 107, is overruled. These concerns go to the weight rather than the admissibility of the statement.

[85] Ocean Bank qualifies this statement, asserting that it used other anti-phishing controls, including three anti-phishing services, and since 2008 has posted various notices regarding account phishing and ACH fraud on the main log-in page to its online banking site for its eBanking customers as well as on the main website. Defendant's Reply SMF ¶ 2; Tarte Decl. ¶¶ 36-37.

D. The May 2009 Allegedly Fraudulent Transactions

In the year 2009, 3,761,327 ACH transactions were sent from the Northern New England Divisions of People's United Bank, including Ocean Bank. Defendant's Additional SMF ¶ 1; Plaintiff's Reply SMF ¶ 1. Between February 13, 2009, and May 6, 2009, Patco successfully logged into its account approximately 107 times. *Id.* ¶ 2. These 107 log-ins represent every time that Patco logged into its eBanking account for any purpose over this time period. *Id.* ¶ 3. The Jack Henry Premium Product risk-scoring engine worked in the background during each of these 107 account activity log-ins. *Id.* ¶ 4.[86] During these 107 log-ins, Patco initiated 12 ACH transactions and was prompted with its challenge questions 12 times. *Id.* ¶ 5. Of these 12 ACH transactions, all but one was for more than $1,000. *Id.* ¶ 6. Specifically, seven of Patco's ACH transactions were for more than $16,000. *Id.* Four were for more than $24,000, and one was for more than $200,000. *Id.* One of Patco's 12 ACH transactions was a $204,724 ACH transfer from Patco's Maine Bank & Trust account to its Ocean Bank checking account. *Id.* ¶ 7. This transfer was initiated on May 3, 2009. *Id.*

On May 6, 2009, one day prior to the first allegedly unauthorized withdrawal, Patco employee Pierce used eBanking to make an ACH transaction in the amount of $16,026.58. *Id.* ¶ 8. Patco's account was set up so that money could be both transferred into or out of Patco's Ocean Bank account. *Id.* ¶ 9. This means that Patco had the capability to, among other things, transfer money from its Ocean Bank account to its account at Maine Bank & Trust. *Id.*[87]

[86] Patco qualifies this statement, denying that the risk-scoring engine triggered any heightened authentication after the Bank lowered the Dollar Amount Rule threshold to $1. Plaintiff's Reply SMF ¶ 4; Suppl. Greene Decl. ¶ 13.

[87] Patco qualifies this statement, asserting that the account arrangement was set up at the recommendation of the Bank for the purpose of transferring deposited funds from the Maine Bank & Trust account into the Ocean Bank account. Plaintiff's Reply SMF ¶ 9; McDowell Dep. at 92-93 (version filed at Docket No. 100-3).

Beginning on May 7, 2009, a series of withdrawals were made on Patco's account over the course of several days. Defendant's SMF ¶ 183; Plaintiff's Opposing SMF ¶ 183. On May 7, 2009, unknown third parties initiated a $56,594 ACH withdrawal from Patco's account. *Id.* ¶ 184. The Bank authenticated this electronic transfer with Patco's company ID and password and Diana Pierce's proper credentials, including her ID, password, and answers to challenge questions. Plaintiff's SMF ¶ 56; Defendant's Opposing SMF ¶ 56. Whoever initiated this transaction did not submit an incorrect password or answers to challenge questions even once. *Id.*[88]

This payment was directed to the accounts of numerous individuals, none of whom had previously been sent money by Patco. *Id.* ¶ 57. The perpetrators logged in from a device unrecognized by Ocean Bank's system, and from an IP address that Patco had never before used. *Id.* ¶ 58. The risk-scoring engine generated a risk score of 790 for the May 7, 2009, transaction. *Id.* ¶ 60. The risk-scoring engine reported the following contributors to the risk score for that transaction: (i) "Very high risk non-authenticated device"; (ii) "High risk transaction amount"; (iii) "IP anomaly"; and (4) "Risk score distributor per cookie age." *Id.* ¶ 61. An RSA manual describing risk score contributors states that any transaction triggering the contributor "Very high risk non-authenticated device" is "a very high-risk transaction." *Id.* ¶ 62. Patco's legitimate transactions generally produced risk scores in the range of 10 to 214, and the documents produced show no prior risk score exceeding 214. *Id.* ¶ 63.[89] Bank personnel did not manually

[88] My recitation incorporates Ocean Bank's qualification.

[89] Ocean Bank qualifies this statement, asserting that it is based on a report showing Patco's log-ins from April 14, 2009, until the alleged fraudulent withdrawals started, because no reports were available for the time period from January 2007 through April 14, 2009. Defendant's Opposing SMF ¶ 63; Suppl. Tarte Decl. ¶ 11.

review the May 7, 2009, transaction. *Id.* ¶ 64. The Bank batched and processed the transaction as usual, and it was paid the next day. *Id.* ¶ 65.[90]

On Friday, May 8, 2009, unknown third parties again successfully initiated an ACH payment order from Patco's account, this time in the total amount of $115,620.26. *Id.* ¶ 66. As with the prior day's transactions, the perpetrators wired money to multiple individual accounts to which Patco had never before sent funds. *Id.* ¶ 67. The perpetrators again used a device that was not, except with regard to the prior day's transaction, recognized by Ocean Bank's system. *Id.* ¶ 68. The payment order originated from the same IP address as the day before. *Id.* ¶ 69. The transaction was larger than any ACH transfer Patco had ever made to third parties. *Id.* ¶ 70.[91] Despite these unusual characteristics, the Bank again batched and processed the transaction as usual, which was paid by the Bank on Monday, May 11, 2009. *Id.* ¶ 71.[92]

On May 11, 12, and 13, unknown third parties initiated further withdrawals from Patco's account in the amounts of $99,068, $91,959, and $113,647, respectively. *Id.* ¶ 72. These transactions involved the sending of money to individuals to whom Patco had never before sent funds, used a device that was not recognized by Ocean Bank's system, and used an IP address that was not recognized as a valid IP address of Patco. Plaintiff's SMF ¶ 73; McDowell Decl.

---

[90] Ocean Bank qualifies this statement, asserting that it did so because the transaction was properly authenticated with Patco's company ID and password and Pierce's credentials, consistent with the Original eBanking Agreement and the Modified eBanking Agreement. Defendant's Opposing SMF ¶ 65; Tarte Decl. ¶ 45; Original eBanking Agreement § XIV; Modified eBanking Agreement § XVI.

[91] Ocean Bank qualifies this statement, asserting that Patco frequently made ACH transactions from its Maine Bank & Trust account to its Ocean Bank checking account that exceeded the amounts of the alleged fraudulent withdrawals, and initiated a $204,724 ACH transfer from its Maine Bank & Trust account on March 3, 2009. Defendant's Opposing SMF ¶ 70; Tarte Decl. ¶ 49; Suppl. Tarte Decl. ¶ 9.

[92] With respect to this transaction, as well, Ocean Bank offers the qualifier that it did so because the transaction was properly authenticated with Patco's company ID and password and Pierce's credentials, consistent with the Original eBanking Agreement and the Modified eBanking Agreement. Defendant's Opposing SMF ¶ 71; Tarte Decl. ¶ 45; Original eBanking Agreement § XIV; Modified eBanking Agreement § XVI. The Bank further qualifies Patco's assertions regarding this transaction by stating that Patco logged into eBanking six times during the week of the allegedly fraudulent withdrawals but failed to notice or to notify the Bank of this allegedly fraudulent transaction at the time. Defendant's Opposing SMF ¶ 67; Tarte Decl. ¶ 46.

¶¶ 9-10; Exh. 16 to Maxwell Dep. (version filed at Docket No. 100-7) at PUB_0013752-55.[93] As a result of these unusual characteristics, these transactions continued to generate higher than normal risk scores. Plaintiff's SMF ¶ 74; Defendant's Opposing SMF ¶ 74.[94] The log-in on May 11, 2009, generated a risk score of 720, while the May 13, 2009, withdrawal generated a risk score of 785. *Id.* ¶ 75. The Bank did not manually review any of these transactions to determine their legitimacy. Plaintiff's SMF ¶ 76; Maxwell Dep. (version filed at Docket No. 100-7) at 131-32.[95]

Portions of the transfers, beginning with the first transfer initiated on May 7, 2009, were returned to the Bank because certain of the account numbers to which the money was slated to be transferred were invalid. Defendant's SMF ¶ 77; Plaintiff's Opposing SMF ¶ 77. As a result, the Bank sent return notices to the home of Mark Patterson, one of Patco's principals, *via* U.S. mail. *Id.* ¶ 78.[96] Patco received the first such notice on the evening of May 13, a full six days after the allegedly fraudulent withdrawals began. *Id.* ¶ 79.[97] The next morning, on May 14, 2009, Patco called the Bank to inform it that Patco had not authorized the transactions. *Id.* ¶ 80. Also on the morning of May 14, another alleged fraudulent transaction was initiated from

[93] Ocean Bank purports to deny paragraph 73, Defendant's Opposing SMF ¶ 73, but its assertions do not contradict it.

[94] Ocean Bank qualifies this statement, asserting that it is based on the limited sample of risk scores available for the period from April 14, 2009, through the time of the alleged fraudulent withdrawals, with RSA reports for the period from January 2007 through April 14, 2009, no longer being available. Defendant's Opposing SMF ¶ 74; Suppl. Tarte Decl. ¶ 11.

[95] The Bank purports to deny this statement, but its denial is in the nature of a qualification: that these ACH transactions were batched only after the Jack Henry Premium Product properly authenticated the transactions with Patco's company ID and password and Pierce's user ID and password and answers to challenge questions. Defendant's Opposing SMF ¶ 76; Tarte Decl. ¶ 45.

[96] Ocean Bank purports to qualify this statement, asserting that Patco chose to have notices sent by mail to Mark Patterson's home. Defendant's Opposing SMF ¶ 78. However, the citations given support only the proposition that Patco chose to have *bank statements* sent to Mark Patterson's home. McDowell Dep. at 77; [Rule] 30(b)(6) Deposition of Patco Construction Company, Inc. (Mark I. Patterson) ("Patterson Dep.") (Docket No. 70), Tab 6 to Appendix, at 49-50.

[97] Ocean Bank admits that Patterson testified to this effect but denies that this was Patco's first notice, asserting that during the week of the fraudulent withdrawals, Patco logged into its eBanking account six times and that, upon log-in, a customer's account balances are conspicuously displayed on the eBanking main page and would have been visible when Patco logged into its account. Defendant's Opposing SMF ¶ 79; Tarte Decl. ¶ 46.

Patco's account in the amount of $111,963. *Id.* ¶ 81. The Bank initially processed this payment order on May 15, 2009. *Id.* ¶ 82.[98] The Bank was able to block a portion of this transaction and recovered a portion of the transferred funds shortly thereafter. *Id.* ¶ 83. Of the total amount withdrawn from Patco's account between May 7 and 15, 2009, Ocean Bank blocked $243,406.83. *Id.* ¶ 84.[99]

Ocean Bank accepted the allegedly fraudulent May 2009 payment orders in compliance with its security procedures. Defendant's SMF ¶ 194; Tarte Decl. ¶ 48.[100] There was no evidence of any security breach on Ocean Bank's systems. Defendant's SMF ¶ 195; Plaintiff's Opposing SMF ¶ 195. Ocean Bank authenticated the May 2009 electronic transfers with Patco's company ID and password and Pierce's proper credentials, including her ID, password, and answers to challenge questions. *Id.* ¶ 196. Whoever perpetrated the alleged fraud knew Patco's company ID and password and Pierce's proper credentials because the person did not submit an incorrect password or incorrect answers to challenge questions even once. *Id.* ¶ 197.

The nature of the Jack Henry application architecture is such that the only place that all authentication credentials can be compromised is on the end-user's computer. *Id.* ¶ 200. Jack Henry's architecture houses the authentication information as encrypted data only and stores parts of it in multiple separate locations (including storing some of the information only on the system of RSA, a different company). *Id.* ¶ 201. This design is such that it would be virtually

[98] Ocean Bank qualifies this statement, asserting that the ACH transactions were only batched after the Jack Henry Premium Product authenticated them with Patco's company ID and password and Pierce's user ID, password, and correct answers to challenge questions. Defendant's Opposing SMF ¶ 82; Tarte Decl. ¶ 45.

[99] My recitation incorporates Ocean Bank's qualification.

[100] Patco purports to deny this statement, but its denial is in the nature of a qualification: that the fraudulent withdrawals were not authenticated by the invisible device ID and the Cyota profiling system because these systems both operated as triggers for challenge questions, and by May 2009 Ocean Bank had configured its system to ask challenge questions on every transaction regardless of the system's recognition of the device used or the risk score associated with the event. Plaintiff's Opposing SMF ¶ 194; Defendant's SMF ¶¶ 84-88; Continued Maxwell Dep. at 33-34, 41.

impossible for someone to garner all of the authentication information without obtaining it from the end-user. *Id.* It has been Jack Henry's experience that virtually all of the fraud incidents involving banks that use Jack Henry products relate back to a compromise of the end-user's machine. *Id.* ¶ 202. Breaching Ocean Bank's systems to obtain Pierce's credentials would have been nearly impossible, as the password was stored encrypted on bank systems, and the challenge question answers were stored at a separate company, Jack Henry/RSA. *Id.* ¶ 203. Patco was the only customer of Ocean Bank that experienced any alleged online banking fraud in May 2009. *Id.* ¶ 205.

Patco did not monitor its eBanking accounts on a daily basis. *Id.* ¶ 206. One of the documented "major duties and responsibilities" of Patco's Accounting Supervisor Diana Pierce, who was primarily responsible for Patco's eBanking, was to "maintain[] summary of weekly cash and cash requirements, allocation of funds between accounts, [and] monitor[] online banking[.]" *Id.* ¶ 207. After a March 2009 reduction in force, Pierce monitored Patco's account sporadically, "maybe a couple times a month[.]" *Id.* ¶ 208.[101] During the week of the fraudulent withdrawals, Patco logged into its eBanking account six times but failed to notice and report the suspicious activity. *Id.* ¶ 209.[102] When a customer logs into eBanking, its account balances are conspicuously displayed on the eBanking main page. *Id.* ¶ 210.[103]

E. Patco's Handling of Its Computers in Wake of Transactions

According to Ocean Bank, on May 14, 2009, immediately after the allegedly fraudulent withdrawals occurred, the Bank instructed Patco to disconnect the computers it used for

[101] My recitation includes, in relevant part, Patco's qualification.
[102] Patco qualifies this statement, asserting that it primarily performed Positive Pay uploads during those six occasions and that logging into eBanking in itself would not provide any indication that fraudulent ACH transactions had taken place. Plaintiff's Opposing SMF ¶ 209; McDowell Dep. at 247-48.
[103] Patco qualifies this statement, asserting that account balance information in itself would not provide any indication that fraudulent transactions had taken place. Plaintiff's Opposing SMF ¶ 210; McDowell Dep. at 247-48.

electronic banking from its network, stop using these computers for work purposes, leave the computers turned on, and bring in a third-party forensic professional or law enforcement to create a forensic image of the computers to determine whether a security breach had occurred. Defendant's SMF ¶ 214; Tarte Decl. ¶ 47. Patco disputes this, stating that a Bank employee recommended only that it check its system for a security breach using a third-party forsensic party, which it attempted to do. Plaintiff's Opposing SMF ¶ 214; McDowell Dep. at 257-58, 262 (version filed at Docket No. 100-3).

Patco did not isolate its computers or forensically preserve the hard drives. Defendant's SMF ¶ 215; Declaration of Edward M. Stroz in Support of Defendant People's United Bank's Motion for Summary Judgment ("Stroz Decl.") (Docket No. 69), Tab 4 to Appendix, ¶ 11.[104] Patco irretrievably altered the computer evidence on the hard drives by (i) failing to take the Pierce and Bramblett computers offline immediately, (ii) allowing Pierce and Bramblett to continue to use their computer during the week following the alleged fraud, and (iii) having an outside IT consultant, Gorham Micro, run anti-malware scans on the Pierce hard drive. Defendant's SMF ¶ 218; Stroz Decl. ¶ 11.[105]

A remnant of Zeus/Zbot malware was found on the Pierce and Bramblett hard drives. Defendant's SMF ¶ 220; Plaintiff's Opposing SMF ¶ 220.[106] However, the Zeus/Zbot malware,

[104] Patco purports to deny this statement, Plaintiff's Opposing SMF ¶ 215, but the McDowell deposition excerpts on which it relies do not controvert that Patco failed to forensically preserve computer hard drives, McDowell Dep. at 263, 277-80 (version filed at Docket No. 100-3). McDowell does testify that Patco isolated Pierce's computer, but indicates that this did not happen until Monday, May 18, 2009. *Id*. at 277-78.

[105] Patco's objection to this statement on the ground that it is conclusory and argumentative, Plaintiff's Opposing SMF ¶ 218, is overruled. Patco alternatively purports to deny this statement, *id*., but the McDowell deposition excerpts and Greene declaration excerpt on which it relies do not controvert it, McDowell Dep. at 262, 279-83 (version filed at Docket No. 100-3); Greene Decl. ¶ 31.

[106] According to Stroz, Zeus software typically "resides on the user's computer and inserts itself into a user's interaction with an online banking website in such a way that the user may be led to believe that he or she is interacting with the legitimate banking website, but, instead, is viewing information supplied by Zeus. Therefore, Zeus can be programmed to display questions similar to the bank's legitimate security questions. The responses to *(continued on next page)*

which contained the encryption key for the Zeus/Zbot configuration file, was quarantined and deleted by the anti-malware scan. *Id.* ¶ 222. Without the encryption key, it is impossible to decrypt the configuration file. *Id.* The configuration file would have identified which banks, if any, the Zeus/Zbot malware would have implicated, if in fact it was of a type that would have intercepted authentication credentials. *Id.* ¶ 223.[107] Without the configuration file, there is no way to tell whether the particular Zeus/Zbot malware version indicated by the remnant on Patco's computer was programmed to intercept online banking credentials. *Id.* ¶ 224.[108] Ocean Bank asserts, and Patco denies, that because the configuration file cannot be decrypted and analyzed to determine whether the Zeus/Zbot was configured with the design to steal Pierce's ACH credentials, it is impossible to say with any certainty that Zeus or another form of malware or something else altogether (*e.g.*, Patco sharing its credentials with a third party) was responsible for the alleged fraudulent withdrawals. *Compare* Defendant's SMF ¶ 225; Stroz Decl. ¶ 22 *with* Plaintiff's Opposing SMF ¶ 225; Greene Decl. ¶ 30.

F. Commercial Reasonableness of Ocean Bank's Security Measures

When the Bank chose its security features, it had to consider not only the threat posed by keyloggers but also threats from various sources including other types of malware such as man-in-the-middle attacks, insider fraud (*e.g.*, employee theft), cyber attacks targeting its online banking application infrastructure, and security breaches of the customer's premises (*e.g.*, theft of tokens, location cameras, intruders). Defendant's Additional SMF ¶ 13; Plaintiff's Reply

---

these questions, as well as other data entered into the page displayed by Zeus, including a user's credentials, can then be sent to a third party and may be stored and used by that third party." Stroz Decl. ¶ 17.

[107] Patco qualifies this statement, asserting that notwithstanding that the configuration file was quarantined and deleted, there is sufficient evidence, including that remnants of a "Zeus Trojan" were found on Patco's machine and that the sequence of events is highly indicative of a Zeus attack, to conclude that it is more likely than not, and indeed highly probable, that the Zeus Trojan was responsible for the fraudulent withdrawals in this case. Plaintiff's Opposing SMF ¶ 223; Greene Decl. ¶ 30.

[108] Patco qualifies this statement, asserting that Zeus generally and most often is used exactly for this purpose. Plaintiff's Opposing SMF ¶ 224; Stroz Decl. ¶ 17.

SMF ¶ 13.[109] Nearly all versions of keylogging malware are able to record data in a log and report it back to the fraudster, who can review it at a later time. *Id.* ¶ 14. The fraudster does not need to be actively monitoring the customer's activity at the time the customer enters the relevant credentials. *Id.* There are thousands of keylogger "drop sites" on the Internet that collect and store credentials for fraudsters to mine and use at a later time. *Id.* This means that, as long as the customer has input his credentials (such as answers to challenge questions) even once into a computer that is compromised by keylogging malware, the fraudster can retrieve those credentials that day, or weeks or even months later. *Id.*[110]

Challenge questions are an excellent form of security against attacks using spoof websites. Defendant's Additional SMF ¶ 15; Suppl. Makohon Decl. ¶ 15. Even in the rare case that a fraudster using a spoof website knows the universe of challenge questions from which the user may select, he or she has no way of knowing which challenge questions the customer has chosen to answer. *Id.* For this reason, fraudsters using spoof websites often prompt users for answers to challenge questions by using generic language such as asking for the answer to "Challenge Question 2," rather than asking the actual challenge questions themselves. *Id.* In contrast, the Bank's security system asks the user the precise challenge question, such as "What is your spouse's middle name?" Defendant's SMF ¶ 16; Suppl. Makohon Decl. ¶ 15. Thus, a customer accustomed to answering challenge questions on the Bank's website is much more

[109] Patco qualifies this statement, asserting that, while it is true that the Bank had to consider other threats, as of 2009 the ability of malicious Trojans to compromise the computers of end-users through keyloggers had become well known, and keyloggers were widely regarded as one of the predominant – if not the predominant – threats facing the online banking community. Plaintiff's Reply SMF ¶ 13; Suppl. Greene Decl. ¶¶ 2, 5, 9, 11.

[110] Patco qualifies this statement, asserting that with a properly configured challenge question system, a fraudster using a keylogger would have to wait until the customer initiated an atypical transaction, and thus triggered the challenge questions, in order to steal the answers to the questions, which should be a very rare occurrence. Plaintiff's Reply SMF ¶ 14; Second Suppl. Greene Decl. ¶ 6.

likely to notice something amiss on a spoof website if he or she is prompted for the answers to challenge questions by generic language. *Id.*[111]

Ocean Bank asserts, based in part on its expert Peter Makohon's opinion, that its security procedures in May 2009 were more than commercially reasonable and provided multifactor authentication and that both the Jack Henry Basic and Premium products were designed to, and did, exceed the recommendations set forth in the FFIEC Guidance, as both products employed multifactor authentication. Defendant's SMF ¶¶ 158-59; Makohon Decl. ¶¶ 10, 17; Edwards Decl. ¶ 22; Tarte Decl. ¶ 42. Based on the opinion of its expert, Sari Greene, Patco denies these assertions. Plaintiff's Opposing SMF ¶¶ 158-59; Greene Decl. ¶¶ 17-26, 32; Suppl. Greene Decl. ¶¶ 2-10, 12-13, 15-16, 33-34.[112]

The parties dispute whether, as Ocean Bank asserts, its security procedures would have been commercially reasonable and complied with FFIEC Guidance as of May 2009, even if the only security feature the Bank had was company IDs and passwords, individual user IDs and passwords, and challenge questions and answers, because such a system constitute multilayered security. *Compare* Defendant's Additional SMF ¶ 26; Suppl. Makohon Decl. ¶ 18 *with* Plaintiff's Reply SMF ¶ 26; Greene Decl. ¶¶ 19-26, 32; Suppl. Greene Decl. ¶¶ 2-10, 12, 15-16, 33-34.[113]

Banks that were using tokens at the time were still experiencing ACH fraud primarily due to security weaknesses on the customers' personal computer and supporting IT infrastructure,

[111] Patco purports to deny paragraphs 15 and 16, but its denial is in the nature of a qualification: that challenge questions that are asked too frequently are not an excellent form of security against attacks using spoof websites. Plaintiff's Reply SMF ¶¶ 15-16; Greene Decl. ¶ 26.

[112] Patco's objection on the ground that the Bank sets forth conclusory opinions on a matter of law, Plaintiff's Opposing SMF ¶¶ 158-59, is overruled with the proviso that the court is indeed the final arbiter on these issues.

[113] Patco's objection on the ground that the Bank sets forth conclusory opinions on a matter of law, Plaintiff's Reply SMF ¶ 26, is overruled with the proviso that the court is indeed the final arbiter on these issues.

and fraudsters were able to compromise a token within seconds of a user entering the token into the bank's web page. Defendant's SMF ¶ 170; Makohon Decl. ¶ 20.[114]

Ocean Bank did not use tokens in May 2009 because it viewed the many security features offered through Jack Henry's Premium Product as more than sufficient to comply with FFIEC Guidance. Defendant's SMF ¶ 171; Plaintiff's Opposing SMF ¶ 171.[115] Tokens were just one more available alternative security option. *Id*. ¶ 172.[116] Moreover, it would have taken Ocean Bank six months or more to roll out tokens to its customer base. *Id*. ¶ 173.

The parties dispute whether, as Ocean Bank asserts, IP blocking and out-of-band authentication would have had little or no impact here, as both have been bypassed by cybercriminals since 2008 and receiving passwords or tokens submitted over out-of-band technologies is not effective, if the passwords are entered into the banking portal through a compromised personal computer. *Compare* Defendant's SMF ¶ 174; Makohon Decl. ¶ 20 *with* Plaintiff's Opposing SMF ¶ 174; Suppl. Greene Decl. ¶¶ 24-26.

The parties also dispute whether, as Ocean Bank asserts, its security procedures in May 2009 were well above the security procedures employed by similarly situated banks at the time. Compare Defendant's SMF ¶ 175; Makohon Decl. ¶ 18 *with* Plaintiff's Opposing SMF ¶ 175; Suppl. Greene Decl. ¶ 33-34.[117] Currently, 50 percent of Jack Henry's financial institutions are

---

[114] Patco purports to deny this statement, Plaintiff's Opposing SMF ¶ 170; however, the cited portions of the declarations of Greene on which it relies qualify, rather than controvert, the statement, with Greene asserting that, while it is true that tokens can be and have been compromised, they still offer increased security over challenge questions alone, Suppl. Greene Decl. ¶ 19.

[115] Patco qualifies this statement, stating that this belief was erroneous. Plaintiff's Opposing SMF ¶ 171; Suppl. Greene Decl. ¶¶ 7-13, 19-21.

[116] Patco's objection to this statement on the basis that it is argumentative and conclusory, Plaintiff's Opposing SMF ¶ 172, is overruled. Patco alternatively qualifies the statement, asserting that, in the words of Jack Henry itself, tokens are "a very secure option that virtually eliminates the risk of an unauthorized user accessing [a] customer's accounts." *Id*.; Exh. 23 to Maxwell Dep. (version filed at Docket No. 100-7) at PUB_0018181.

[117] Patco's objection to this statement on the ground that it sets forth a conclusory opinion that is nothing more than Ocean Bank's expert's opinion and is lacking in foundation, Plaintiff's Opposing SMF ¶ 175, is overruled. In general, an expert's opinion is the proper subject of a statement of material facts. In addition, in the cited portion of

(continued on next page)

using the Premium Product. Defendant's SMF ¶ 176; Plaintiff's Opposing SMF ¶ 176. Nine percent of Jack Henry's financial institutions use the Premium Product with the out-of-band option. *Id.* ¶ 177. Forty-one percent of Jack Henry's financial institutions use the Basic Product. *Id.* ¶ 178.[118]

The parties dispute whether, as Ocean Bank asserts, its security procedures exceeded those recommended in the FFIEC Guidance. *Compare* Defendant's SMF ¶ 179; Makohon Decl. ¶ 17 *with* Plaintiff's Opposing SMF ¶ 179; Suppl. Greene Decl. ¶¶ 2-10, 12-13, 15-16, 33-34.[119] Ocean Bank employed SSL encryption, a security method not even employed by $700 billion bank Wachovia, in May 2009. Defendant's SMF ¶ 180; Plaintiff's Opposing SMF ¶ 180.[120] Ocean Bank used Jack Henry's Premium Product, which employed adaptive authentication similar to that used by much larger national bank Wachovia. *Id.* ¶ 181.[121] Patco's own expert admitted in an email to Patco that Ocean Bank's procedures were commercially reasonable. Defendant's SMF ¶ 182; Tab 18 (Docket No. 71) to Appendix.[122]

---

the Makohon declaration, Makohon sets forth reasons for his opinion, for example, that, in May 2009, hundreds of other small to regional-sized banks used the Basic Product and many used products less sophisticated than either the Premium or Basic product. Makohon Decl. ¶ 18.

[118] Patco qualifies paragraphs 176 through 178, asserting that they do not account for what other authentication procedures, such as tokens, out-of-band procedures, and manual reviews, might be in place at other banks using the Jack Henry products, or those banks' configuration of the Jack Henry products. Plaintiff's Opposing SMF ¶¶ 176-78; Greene Decl. ¶ 35.

[119] Patco's objection on the ground that the Bank sets forth conclusory opinions on a matter of law, Plaintiff's Opposing SMF ¶ 179, is overruled with the proviso that the court is indeed the final arbiter on this issue.

[120] Patco qualifies this statement, asserting, in relevant part, that SSL encryption is commonly used, relatively inexpensive, and not intended to protect against keylogging malware. Plaintiff's Opposing SMF ¶ 180; Suppl. Greene Decl. ¶ 17.

[121] Patco qualifies this statement, asserting that the two most important features of the Premium Product system, the device ID system and risk-scoring engine, were deprived of any practical utility after the Bank configured its system to ask challenge questions on every transaction, and that there were critical differences between the authentication procedures employed by the Bank and those employed by Wachovia; for example, Wachovia used tokens. Plaintiff's Opposing SMF ¶ 181; Defendant's SMF ¶¶ 84-88; Continued Maxwell Dep. at 33-34, 41; Deposition of Peter A. Makohon (Docket No. 75-10) at 137-38.

[122] Patco purports to deny this statement, Plaintiff's Opposing SMF ¶ 182, but the cited portions of the Greene declaration on which it relies qualify, rather than controvert, the underlying statement, Suppl. Greene Decl. ¶¶ 29-30 (explaining, *inter alia*, that Greene's comment that it appeared that the Bank had instituted generally accepted

(continued on next page)

III. Discussion

Patco brings six claims against Ocean Bank seeking to recover sums withdrawn from its account as a result of the series of allegedly fraudulent transactions in May 2009 as well as interest assessed by the Bank on that portion of a Patco line of credit tapped by the Bank to help cover the allegedly fraudulent withdrawals. *See generally* Second Amended Complaint ("Complaint") (Docket No. 39). Specifically, Patco brings claims pursuant to UCC § 4A-201 *et seq*. (Count I), negligence (Count II), breach of contract (Count III), breach of fiduciary duty (Count IV), unjust enrichment (Count V), and conversion (Count VI). *See id*. ¶¶ 49-82. The parties cross-move for summary judgment on Count I, and Ocean Bank moves for summary judgment on the remaining claims on grounds that Article 4A provides the exclusive remedy for unauthorized electronic funds transfers and, alternatively, none of those counts survives summary judgment on its merits. *See* Defendant's S/J Motion at 1-4; Plaintiff's S/J Motion at 1. For the reasons that follow, I recommend that Ocean Bank's motion for summary judgment be granted and that of Patco denied.[123]

A. Count I (UCC Article 4A)

1. Background

The allocation of loss involving commercial electronic funds transfers is governed, *inter alia*, by Article 4A of the UCC, first approved by the National Conference of Commissioners on Uniform State Laws and the American Law Institute in 1989. *See, e.g.*, Robert W. Ludwig, Jr., Salvatore Scanio, & Joseph S. Szary, *Malware and Fraudulent Electronic Funds Transfers: Who*

banking practices for high risk transactions was preliminary and based on limited information, without benefit of review of how the Bank's security procedures were actually configured and implemented).

[123] The parties disagree whether Maine or Connecticut law applies. *Compare* Defendant's SMF ¶ 61 (Connecticut law) *with* Plaintiff's Opposing SMF ¶ 61 (Maine law). I need not resolve the dispute because, under either state's laws, the outcome is the same.

Bears the Loss?, 16 Fidelity L.J. 101, 106 (Oct. 2010). "Before [Article 4A] was drafted there was no comprehensive body of law – statutory or judicial – that defined the juridical nature of a funds transfer or the rights and obligations flowing from payment orders." Conn. Gen. Stat. Ann. § 42a-4A-102 cmt.; 11 M.R.S.A. § 4-1102 cmt. Article 4A's drafters explained:

> In the drafting of Article 4A, a deliberate decision was made to write on a clean slate and to treat a funds transfer as a unique method of payment to be governed by unique rules that address the particular issues raised by this method of payment. A deliberate decision was also made to use precise and detailed rules to assign responsibility, define behavioral norms, allocate risks and establish limits on liability, rather than to rely on broadly stated, flexible principles. In the drafting of these rules, a critical consideration was that the various parties to funds transfers need to be able to predict risk with certainty, to insure against risk, to adjust operational and security procedures, and to price funds transfer services appropriately. This consideration is particularly important given the very large amounts of money that are involved in funds transfers.

Id.

Of critical importance to the instant case is Article 4A-202, which provides, in relevant part:

> If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer.

Conn. Gen. Stat. Ann. § 42a-4A-202(b); *see also* 11 M.R.S.A. § 4-1202(2). For purposes of Article 4A:

> "Security procedure" means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar

> security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure.

Conn Gen. Stat. Ann. § 42a-4A-201; *see also* 11 M.R.S.A. § 4-1201.

Pursuant to these provisions, Patco, rather than the Bank, bore the risk of loss flowing from the allegedly unauthorized May 2009 transactions if (i) Patco and the Bank agreed to a security procedure, (ii) the security procedure was commercially reasonable, and (iii) the Bank accepted the payment orders in question in good faith and in compliance with the security procedure and any relevant written agreement or instruction of Patco.[124]

2. Whether Parties Agreed to Security Procedure and Bank Complied Therewith

The central issue in this case is whether the Bank's security procedures were commercially reasonable. *See, e.g.*, Plaintiff's S/J Motion at 10 ("Liability against the Bank is proper under Article 4A because the Bank did not maintain commercially reasonable security procedures to protect Patco's accounts from theft in May of 2009, when the unauthorized withdrawals occurred."). Patco does not argue, either in support of its own motion for summary

[124] As Patco points out, *see* Plaintiff's S/J Motion at 13, a customer may yet avoid liability, even if these three tests are met, by showing either that (i) the bank agreed to take all or part of the loss resulting from an unauthorized payment order, or (ii) the information used to effect the fraudulent payment order was not obtained, either directly or indirectly, from the customer or someone under the customer's control, *see* Conn. Gen. St. Ann. § 42a-4A-203(a); 11 M.R.S.A. § 4-1203(1). Patco does not claim that either of these exceptions applies in this case. Rather, it cites this provision for the proposition that this is the only point in the statutory analysis at which an examination of the *customer's* security procedures may be appropriate. *See* Plaintiff's S/J Motion at 13-14. As the Bank points out, *see* Defendant's S/J Motion at 20-22, a security procedure is *deemed* commercially reasonable if "(i) the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and (ii) the customer expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer[,]" Conn. Gen. St. Ann. § 42a-4A-202(c); *see also* 11 M.R.S.A. § 4-1202(3). Ocean Bank does argue, in the alternative, that its security procedures should be deemed commercially reasonable because it offered Patco the availability of emailing alerting, and Patco did not avail itself of that offer. *See* Defendant's S/J Motion at 20-22. Nonetheless, as Patco points out, *see* Opposition to Defendant's Motion for Summary Judgment ("Plaintiff's S/J Opposition") (Docket No. 99) at 18-19, there is no dispute that Patco was unaware of this offer, which was posted online, and hence Patco cannot be said to have "refused" it, *see* Defendant's SMF ¶ 126; Plaintiff's Opposing SMF ¶ 126. Further, as Patco notes, *see* Plaintiff's S/J Opposition at 19-20, there is no evidence that it expressly agreed in writing to be bound by a security procedure that *it* had chosen following Ocean Bank's "offer" of email alerting.

judgment or in opposition to that of the Bank, that the Bank failed to act in good faith and in compliance with its security procedures when it processed the allegedly fraudulent transfers. Indeed, the undisputed evidence is that the Bank processed those transfers only after its system authenticated that the proper IDs, passwords, and answers to challenge questions were provided. *See, e.g.*, Defendant's SMF ¶¶ 196-97; Plaintiff's Opposing SMF ¶¶ 196-97.

While, in its motion for summary judgment, Patco argued in the alternative that it did not agree to a security procedure, or that those few security procedures to which it did agree, standing alone, were not commercially reasonable, *see* Plaintiff's S/J Motion at 31-34, it did not specifically respond, either in its reply memorandum or in its opposition to the Bank's motion for summary judgment, *see generally* Plaintiff's S/J Opposition; Plaintiff's Reply to Defendant's Opposition to Plaintiff's Motion for Summary Judgment ("Plaintiff's S/J Reply") (Docket No. 109), to the Bank's argument that Patco *did* agree, expressly and/or implicitly, to the full panoply of security measures implemented by the Bank, *see* Defendant's S/J Motion at 14; Defendant People's United Bank's Opposition to Plaintiff Patco Construction Company, Inc.'s Motion for Summary Judgment ("Defendant's S/J Opposition") (Docket No. 88) at 7-10.[125] Patco's silence in the face of this argument fairly can be construed as conceding the point. *See, e.g., Grenier v. Cyanamid Plastics, Inc.*, 70 F.3d 667, 678 (1st Cir. 1995) ("If a party fails to assert a legal reason why summary judgment should not be granted, that ground is waived and cannot be considered or raised on appeal.") (citations and internal quotation marks omitted).

In any event, even assuming *arguendo* that Patco did not impliedly concede the point, there is no genuine dispute that it agreed to the core security procedures visible to users that

[125] Patco did incorporate its motion for summary judgment by reference into both its reply memorandum and its opposition to the Bank's motion for summary judgment. *See* Plaintiff's S/J Reply at 1; Plaintiff's S/J Opposition at 1. Nonetheless, it did not address the Bank's specific arguments.

comprised the key components of the integrated security package used by the Bank. Patco expressly agreed to the use of security passcodes, which consisted of a customer ID and customer password and a user ID and user password for each authorized user of the customer, *see* Defendant's SMF ¶ 145; Plaintiff's Opposing SMF ¶ 145, and it agreed by course of performance to the use of challenge questions, having cooperated in setting up answers to such questions and having answered them in the course of conducting eBanking, *see id.* ¶¶ 146-47; *Leshine Carton Co. v. Matik N. Am.*, No. CV0540076365, 2006 WL 1359651, at *1 (Conn. Super. Ct. Mar. 9, 2006) ("[T]he UCC parol evidence rule permits contract terms to be explained or supplemented (a) by course of dealing or usage of trade as provided by § 42a-1-205 or by course of performance as provided by § 42a-2-208; and (b) by evidence of consistent additional terms.") (citation and internal quotation marks omitted); 11 M.R.S.A. §§ 1-1201(3), 1-1303(1) (same); *Regatos v. North Fork Bank*, 257 F. Supp.2d 632, 646 (S.D.N.Y. 2003) (for purposes of Article 4A, commercial customer and bank agreed on security procedure when, regardless of whether there was an explicit agreement, their unvaried course of conduct over a period of four years evinced a clear understanding on security procedure).

While other aspects of the Premium Product security system, such as device authentication, IP Geo location, transaction monitoring, and the risk-profiling engine, were invisible to Patco, they were integrated with, and largely operated in the service of, the visible portions of the system. Thus, Patco fairly can be said to have agreed to the use of the Premium Product security system *in toto*.

In addition, by virtue of the posting online of the Modified eBanking Agreement, Patco effectively agreed to monitor its commercial accounts daily. While Patco protests that it did not actually ever see the Modified eBanking Agreement and thus was never properly notified of its

existence or bound by it, *see* Plaintiff's S/J Opposition at 21-22, the Bank reserved the right, in the Original eBanking Agreement, to modify the terms and conditions of that agreement at any time effective upon publication, see Defendant's SMF ¶ 24; Plaintiff's Opposing SMF ¶ 24. There is no dispute that Patco reviewed and agreed to the terms of the Original eBanking Agreement. *See id*. ¶¶ 14-18. The online publication of the Modified eBanking Agreement hence was binding upon Patco. *See, e.g., Harold H. Huggins Realty, Inc. v. FNC, Inc*., 575 F. Supp.2d 696, 708 (D. Md. 2008) (unilateral modification of Internet-based service contract held effective when prior agreements permitted modification at any time and stated that modifications would be effective after they were posted for 30 days).[126]

The agreed-to obligation of Patco, a commercial banking customer, to monitor its accounts daily in turn fits the definition of a "security procedure": "a procedure established by agreement of a customer and a receiving bank for the purpose of . . . detecting error in the transmission or the content of the payment order or communication." Conn Gen. Stat. Ann. § 42a-4A-201; 11 M.R.S.A. § 4-1201.[127]

3. Whether the Procedure Was Commercially Reasonable

Article 4A provides, in relevant part:

> Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and

[126] Patco cites *Douglas v. United States Dist. Court for Cent. Dist. of Cal.*, 495 F.3d 1062, 1066 (9th Cir. 2007), for the proposition that generic online publication constitutes insufficient notice to create a binding modification of an agreement. *See* Plaintiff's S/J Opposition at 21. *Douglas* is distinguishable. In *Douglas*, the court held that an individual who had entered into a contract with America Online ("AOL") for long-distance telephone service was not bound by a revised contract that AOL's successor, Talk America, had posted on its website. *See Douglas*, 495 F.3d at 1066-67. However, there is no suggestion that the individual had entered into an agreement with AOL providing for modification of that agreement upon online posting by AOL. *See id*.

[127] To the extent that Patco or its experts argue that this obligation pertained only to ACH debit transactions, not ACH credit transactions such as the fraudulent withdrawals at issue, *see* Plaintiff's S/J Opposition at 22, I disagree. Although the monitoring obligation was set forth in the context of ACH debits, it is an unambiguous obligation to monitor all commercial accounts daily. *See* Defendant's SMF ¶ 38; Plaintiff's Opposing SMF ¶ 38.

> frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated.

Conn. Gen. Stat. Ann. § 42a-4A-202(c); 11 M.R.S.A. § 4-1202(3).

In official commentary, the drafters of Article 4A have further illuminated the concept of "commercial reasonableness" as follows:

> The burden of making available commercially reasonable security procedures is imposed on receiving banks because they generally determine what security procedures can be used and are in the best position to evaluate the efficacy of procedures offered to customers to combat fraud. The burden on the customer is to supervise its employees to assure compliance with the security procedure and to safeguard confidential security information and access to transmitting facilities so that the security procedure cannot be breached.
>
> ***
>
> The concept of what is commercially reasonable in a given case is flexible. Verification entails labor and equipment costs that can vary greatly depending upon the degree of security that is sought. A customer that transmits very large numbers of payment orders in very large amounts may desire and may reasonably expect to be provided with state-of-the-art procedures that provide maximum security. But the expense involved may make use of a state-of-the-art procedure infeasible for a customer that normally transmits payments orders infrequently or in relatively low amounts. Another variable is the type of receiving bank. It is reasonable to require large money center banks to make available state-of-the-art security procedures. On the other hand, the same requirement may not be reasonable for a small country bank. A receiving bank might have several security procedures that are designed to meet the varying needs of different customers. The type of payment order is another variable. For example, in a wholesale wire transfer, each payment order is normally transmitted electronically and individually. A testing procedure will be individually applied to each payment order. In funds transfers to be made by means of an automated clearing house many payment orders are incorporated into an electronic device such as a magnetic tape that is physically delivered. Testing of the individual payment orders is not feasible. Thus, a different kind of security procedure must be adopted to take into account the different mode of transmission.
>
> The issue of whether a particular security procedure is commercially reasonable is a question of law. Whether the receiving bank complied with the procedure is a question of fact. It is appropriate to make the finding concerning commercial reasonability a matter of law because security procedures are likely to be standardized in the banking industry and a question of law standard leads to more

> predictability concerning the level of security that a bank must offer to its customers. The purpose of subsection (b) is to encourage banks to institute reasonable safeguards against fraud but not to make them insurers against fraud. A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge deciding the question would have opted for a more stringent procedure. The standard is not whether the security procedure is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank, which is a lower standard. On the other hand, a security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank should not be held to be commercially reasonable.

Conn. Gen. St. Ann. § 42a-4A-203 cmts. 3-4; 11 M.R.S.A. § 4-1203 cmts. 3-4.

If, pursuant to these provisions, a bank is judged to bear the risk of loss, it must refund to its customer, with interest, any amounts retained to fund the fraudulent payment orders. *See* Conn. Gen. St. Ann. § 42a-4A-204; 11 M.R.S.A. § 4-1204(1).

a. Patco's Arguments

Patco seeks summary judgment in its favor as to Count I, and opposes the Bank's bid for summary judgment on that count, on the bases that (i) the Bank made a crucial error when it set the Dollar Amount Rule threshold at $1, effectively creating a "single-factor" authentication system that was ineffective against the known threat of compromise of an end-user's computer by keylogging malicious software, and (ii) the Bank failed to implement additional measures, such as tokens or a true out-of-band option, that would have increased the effectiveness of its security procedures. *See* Plaintiff's S/J Motion at 16-31; Plaintiff's S/J Opposition at 2-18.

i. The Lowering of the Dollar Amount Rule Threshold to $1

Patco points out that the Bank's core security procedures in May 2009 consisted of the use of IDs, passwords, and challenge questions. *See* Plaintiff's S/J Opposition at 2.[128] Patco's

[128] The arguments set forth in Patco's opposition to the Bank's motion for summary judgment largely echo and refine those set forth in its own motion for summary judgment. Accordingly, I have cited primarily to its opposing brief.

device identification system, cookies, transaction monitoring, risk-scoring systems, and IP Geo location tracking all served merely as alternative bases for the triggering of challenge questions. *See id*. at 2 n.1.

In June 2008, according to Patco expert Sari Greene, the Bank made a crucial error in configuring its system when it set the Dollar Amount Rule threshold at $1. *See id*. at 3. Instead of enhancing security, as the Bank wrongly believed, this change undermined the effectiveness of the challenge questions as a security procedure. *See id*. This was so, according to Patco and Greene, because the frequent asking of such questions increased the risk that a fraudster using "keylogger" malicious software could intercept answers to such questions. *See id*. at 3-4. If a fraudster attempting to gain access to a customer's account had obtained only a user's ID and password, other components of the Jack Henry Premium Product designed to recognize aberrant activity, such as the IP Geo tracking and risk-scoring systems, would trigger the challenge questions, which the fraudster then would be unable to answer. *See id*. at 4-5.

Patco does not dispute, as the Bank's expert Peter Makohon points out, that a computer infected with keylogging malware will capture the answers to challenge questions if they are used even once. *See id*. at 5-6. But Patco posits that the timing matters: if legitimate users trigger challenge questions only rarely, a fraudster's ability to compromise the user's account could be delayed for months, years, or even indefinitely, during which time, for example, the malware might be detected and eliminated by a customer's antivirus software, or the fraudster might give up and move to another target or be brought to justice. *See id*. at 6-7 & n.5.[129]

[129] This represents a shift from Patco's earlier position, expressed in its motion for summary judgment, that if a security system were properly configured to ask challenge questions only infrequently, "[f]raud . . . could only be achieved if the keylogger happened to be present on the customer's computer and the fraudster happened to be monitoring the customer's activity on the rare occasion the customer himself might initiate an atypical transaction, thus prompting the challenge questions." Plaintiff's S/J Motion at 19.

Beyond this, Patco challenges the Bank's logic in lowering the Dollar Amount Rule threshold to $1 on account of asserted low-dollar-amount ACH fraud, asserting that, regardless of the Dollar Amount Rule threshold, the Bank's system was configured to pose challenge questions based on other indicia of fraud, such as an unrecognized IP address, and thus, challenge questions would have been triggered in the event of fraudulent activity regardless of the Dollar Amount Rule threshold. *See id*. at 7. Indeed, Patco notes, the individuals perpetrating the alleged 2008 frauds were asked, and successfully answered, challenge questions. *See id*. Thus, it reasons, the lowering of the Dollar Amount Rule threshold added no additional protection even in cases of asserted low-dollar amount fraud. *See id*. at 7-8.

Patco argues that, to the extent that the Bank and Jack Henry believed that the setting of the Dollar Amount Rule threshold had no bearing on the effectiveness of the security system, they were wrong. *See id*. at 10-11. RSA Security had recognized this fact when it warned financial institutions to edit decision rules carefully, slowly, and with great caution because such rules play a major role in fraud prevention. *See id*. Moreover, Patco notes, the Bank's position is contradicted by its own argument that it lowered the Dollar Amount Rule threshold to foil fraudsters engaged in low-dollar amount thefts. *See id*. at 11 n.9.

Patco states that, in May 2009, it was virtually universally recognized, as it is today, that a system offering a level of protection no greater than user IDs and passwords alone was not commercially reasonable for high-risk transactions. *See id*. at 5.[130] Patco argues that the Bank's system, as configured, was not effectively a "multifactor" authentication system in May 2009

[130] Patco explains that, although its expert Sari Greene did state in an email to it on May 26, 2009, the same day she had been formally retained, that the Bank's security seemed to conform to generally accepted banking practices, she was not aware at that time that the Bank had configured its system to ask challenge questions on every transaction and had not been given specific information about the underlying technical characteristics of the Bank's authentication security procedures. *See* Plaintiff's S/J Opposition at 5 n.3.

because a fraudster needed only two things to access a commercial account through the Bank's eBanking website: (i) the customer's user ID/password combinations and (ii) the answers to the customer's challenge questions. *See id.* at 13. Patco asserts that this information comprised a single factor: something the user knew. See id. Patco argues that the Bank's invisible device ID (the asserted second factor) and profiling engine (the asserted third factor) acted only as triggers for the challenge questions (part of the first factor) rather than, for example, resulting in denial of access to the system. *See id.*

More to the point, Patco reasons, the Bank deprived the invisible device ID and the profiling engine of any practical effect whatsoever by configuring the Dollar Amount Rule threshold at $1. *See id.* at 14. Patco asserts that, even if the Bank's system had possessed some semblance of multifactor authentication when first implemented by Jack Henry, the Bank had effectively turned off both allegedly multifactor components of the system prior to May 2009. *See id.* at 15.[131]

As a result of the Bank's configuration of its security system, Patco reasons, that system in May 2009 was ineffective against a by-then-well-known threat, the compromise of end-users' computer systems by keylogging malware. *See* Plaintiff's S/J Opposition at 11-12. The Bank's security procedures, in Patco's view, accordingly were not commercially reasonable. *See id.* at 12.

[131] Patco also argues, in its motion for summary judgment, that the Bank's security procedures failed to take into account the known circumstances of Patco because, although the allegedly unauthorized withdrawals were completely different from those typically made by Patco, the Bank paid no attention to the discrepancies, having configured its system in such a way that its own risk profiling was ineffective to prevent fraud and having failed to adopt another security procedure that would reveal the discrepancies, such as manual review. *See* Plaintiff's S/J Motion at 23-27. Patco argues, "Inaction in the face of potential fraud is not the mark of a commercially reasonable security procedure." *Id.* at 26. Patco also contends that the Bank permitted its ACH withdrawal limit to be set at an imprudently high level without warning it of the security risks in so doing. *See id.* at 26-27. Even assuming *arguendo* that the Bank had a duty to warn Patco of such risks and that, had Patco been warned, it would have requested an ACH limit that would have lessened its loss, ACH limits do not comprise a "security procedure" for purposes of Article 4A and, thus, have no bearing on the instant analysis.

ii. Security Measures Not Implemented by Ocean Bank

Patco further argues that the Bank neglected to implement "security procedures in general use by customers and receiving banks similarly situated[,]" Conn. Gen. St. Ann. § 42a-4A-202(c); 11 M.R.S.A. § 4-1202(3), a factor cutting against a finding of commercial reasonableness, when it failed to adopt additional security measures such as tokens and "true" out-of-band authentication, *see* Plaintiff's S/J Motion at 27-31; Plaintiff's S/J Opposition at 15-18. Patco argues that:

1. By May 2009, Internet banking security had largely moved to hardware-based tokens and other means of generating "one-time" passwords. *See* Plaintiff's S/J Motion at 28. As of then, both People's United Bank and Wachovia, which employed Makohon, were using tokens for commercial accounts, as were many community banks in New England. *See id*. at 29. Although tokens can be compromised, bypassing them requires greater sophistication than obtaining challenge questions. *See* Plaintiff's S/J Opposition at 16. The fraudster must use the information within seconds of acquiring it, before the system generates a new password to replace the old. *See id*. The answers to challenge questions, by contrast, may be used at the fraudster's leisure, particularly when, as was the case at Ocean Bank, the answers are static. *See id*. at 16 & n.16. Even if a token had been used and compromised in this case, the magnitude of the resulting fraud would have been greatly reduced because the captured password could not have been used after the initial transaction. *See id*. at 16.

2. Of banks that did not use tokens in May 2009, many community banks in New England used some form of out-of-band verification or conducted manual reviews of uncharacteristic or suspicious transactions. *See* Plaintiff's S/J Motion at 29. Although the Bank's expert, Makohon, states that receiving passwords or tokens over out-of-band

technologies is not effective if the passwords are entered into the banking portal using a compromised personal computer, true out-of-band authentication entails entering information through the out-of-band channel itself. *See* Plaintiff's S/J Opposition at 17. Even if Jack Henry did not offer a true out-of-band option in May 2009, others did. *See id.* Moreover, even Jack Henry's product offered greater security because it entailed the generation of a one-time password. *See id.*

3. Ocean Bank failed to conduct manual reviews of suspicious transactions in May 2009, although it could have done so. *See id.* at 18. Ocean Bank began reviewing reports at the end of 2009. *See id.* at 29.

b. Ocean Bank's Arguments

Ocean Bank seeks summary judgment as to Count I on the ground that its security measures in place as of May 2009 met the standard of commercial reasonableness, given that:

1. Patco expressed no wishes to the Bank regarding security procedures apart from those contained in the parties' agreements. *See* Defendant's S/J Motion at 15-16.[132]

2. The Bank's security procedures took into account the circumstances of the customer known to the Bank by building a risk profile based on the customer's eBanking habits, with the system comparing each transaction against that auto-generated profile, and the Bank set Patco's ACH withdrawal limit based on its specific needs. *See id.* at 16.

3. The Bank made email alerts available to Patco, but Patco chose not to use them.

[132] To the extent that Patco asserts, in a footnote in its motion for summary judgment, that it requested email notification upon the transfer of monies from its Ocean Bank accounts, *see* Plaintiff's S/J Motion at 31 n.45, the Bank succeeds in demonstrating that there is no genuine issue of material fact that this request, made in 2004, was not a request for email alerts with respect to eBanking, which were not offered by the Bank until 2006, *see* Defendant's S/J Opposition at 11.

See id.[133]

4. The Bank's security procedures exceeded those in general use by customers and similarly situated banks in May 2009, as well as those suggested by the FFIEC Guidance, the Bank having (i) chosen to implement the Jack Henry Premium multifactor authentication system, which incorporated not only multiple "factors" but also layered security, and (ii) employed numerous other controls to reduce the risk of account fraud and identity theft, including SSL encryption, the use of commercial third-party anti-phishing services, the use of transaction-based email alerting, and the use of cyber intelligence from RSA's eFraud Network. *See id*. at 16-18. Further, the Bank contends, it periodically changed the transaction threshold at which challenge questions were asked to adapt to the changing threat landscape, for example, lowering the Dollar Amount Rule threshold in response to instances of ACH fraud. *See id*. at 18.

The Bank argues that, in the face of this strong evidence, Patco resorts to offering suggestions for how the Bank's security measures could have been improved, for example, how it should have configured its Dollar Amount Rule threshold and what other measures it should have implemented. *See* Defendant People's United Bank's Reply Memorandum in Support of Its Motion for Summary Judgment ("Defendant's S/J Reply") (Docket No. 116) at 1-2. The Bank contends that these assertions miss the critical question, which is not whether the Bank had the best system available, or whether a different system would have been better or would have prevented the fraud, but, rather, whether the procedures the Bank *did* use were commercially reasonable. *See id*. at 2-3.

[133] Patco adduces evidence that it received no individual notification of the availability of email alerts and was unaware of the existence of that option. *See* Plaintiff's Opposing SMF ¶ 120. Nonetheless, the Bank posted notice of the availability of such alerts online, and a user only had to click on a tab visible on the eBanking webpage to begin the process of setting up such alerts. *See* Defendant's SMF ¶¶ 128-29. By posting the availability of email alerting in several formats online, the Bank sufficiently notified Patco of its availability.

The Bank argues that, in any event, Patco's theory that the Bank configured the Dollar Amount Rule threshold in such a manner as to compromise the Jack Henry system and cause the fraud at issue is fundamentally flawed. *See id*. at 3-5.

First, the Bank argues, the premise that keylogging caused the fraud in question is based on pure supposition, Patco having irreparably altered the evidence on its hard drives by running scans on its computers and continuing to use them prior to making proper forensic copies. *See id*. at 3. Thus, the Bank reasons, no one can know for certain when or whether keylogging malware infected Pierce's computer and enabled the alleged fraud. *See id*. at 4.

Second, the Bank contends, even accepting that keylogging was the culprit, Patco retreated from the premise set forth in its motion for summary judgment that a keylogger must be online at the same time that a user is inputting data in order to capture that data. *See id*. at 4. Patco instead offers what the Bank terms "remote hypothetical scenarios" in which keyloggers would be delayed and possibly frustrated in stealing or using challenge questions if such questions were asked infrequently. *See id.* at 4-5.

Third, the Bank argues that even if the Dollar Amount Rule threshold had been set at a higher amount, for example, the Jack Henry default setting of $1,000 or even as high as $16,000, this would not have materially changed the frequency with which Patco was prompted to answer its challenge questions. *See id.* at 5. Patco generally made ACH transactions well over $1,000 and often in excess of $16,000. *See id*.

Fourth, the Bank asserts that Patco's contention that its Jack Henry Premium Product as configured was not a "true" multifactor authentication system is wrong. *See id*. at 5-6 n.5. The Bank points out that there is no dispute that the system incorporated such aspects as an invisible device ID and a risk-scoring module. *See id*. It argues that Patco, in essence, attempts to

manufacture an additional "requirement" for multifactor authentication, unsupported in the FFIEC Guidance or in the caselaw, by arguing that the system must *respond* in a certain way to each of the factors, for example, by blocking a transaction if one of the factors fails. *See id*. Moreover, it notes, Patco's assertion that the system's only response in all situations was to trigger challenge questions is factually wrong: if the system detected activity matching suspicious activity reported to the eFraud Network, the transaction was immediately blocked. *See id*.

In any event, the Bank contends, even if its system properly could be characterized as "single factor" as of May 2009, the FFIEC Guidance did not require multifactor authentication but, rather, stated that "where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks." *Id*. (quoting FFIEC Guidance at 1-2). The Bank notes that its security procedures were multilayered in that they employed challenge questions as well as IDs/passwords, and that it employed other controls such as SSL encryption, an eFraud Network subscription, commercial third-party anti-phishing services, posting of fraud alerts on its website, and email alerting. *See id*.

Finally, the Bank argues, its non-implementation, as of May 2009, of security procedures such as tokens, manual review, and out-of-band authentication does not render the security procedures that it did use commercially unreasonable. *See* Defendant's S/J Opposition at 3. It points out that less than 2 percent of the 1,500 banks that Jack Henry serviced in any capacity used tokens in May 2009. *See id*. It notes that it concluded that Jack Henry's out-of-band authentication option would have offered little to no benefit in overall security. *See id*. at 19. It observes that Jack Henry's system did not require manual review and, in any event, Patco itself

logged into its account six times during the week of the allegedly fraudulent withdrawals without detecting the alleged fraud. *See id*. at 20.

c. Analysis

This is a hard-fought and well-presented case bearing on a discrete but nuanced issue. There is a relatively small body of caselaw construing Article 4A. The parties point to no case considering whether the configuration of a discretionary rule can render a bank's security system commercially unreasonable, and my research discloses none.

Patco makes a facially appealing argument that, in setting the Dollar Amount Rule threshold at $1, the Bank ill-advisedly neutralized critical aspects of the seemingly high-quality security system it chose to implement in the wake of the issuance of the FFIEC Guidance. Yet, for the reasons that follow, I conclude that the Bank has the better argument and has demonstrated that the security procedures that it had in place as of May 2009 were commercially reasonable.

The Jack Henry Premium Product was the result of a careful effort at compliance with the 2005 FFIEC Guidance. The Bank's affiliate, Chittenden Bank, recognized that the Jack Henry NetTeller product involved high-risk transactions that required multifactor authentication and worked with Jack Henry, which in turn worked with RSA/Cyota, to create such a security system. *See* Plaintiff's SMF ¶ 23; Defendant's Opposing SMF ¶ 23; Defendant's SMF ¶ 71; Plaintiff's Opposing SMF ¶ 71. The Premium Product employed by the Bank, marketed at the time as "the most robust and effective solution available," Defendant's SMF ¶ 73; Plaintiff's Opposing SMF ¶ 73, is a multifactor authentication system, relying on at least two factors: something the user knows (ID and password) and something the user has (device identification specific to the user's personal computer and its use of the bank's application). On its face, the

Premium Product, when measured against the FFIEC Guidance yardstick that both parties have treated as a critical factor in this case, is commercially reasonable, incorporating not only at least two factors but also multiple layers (challenge questions in addition to passwords/IDs). Indeed, Patco's expert, Sari Greene, so concluded upon her preliminary review of the Bank's security system. *See id.* ¶ 182.

Further, the Premium Product provided additional security measures, including a subscription to the eFraud Network, *see, e.g., id.* ¶¶ 121-22, and the Bank chose to implement measures above and beyond those provided through the Premium Product, such as making email alerts available and requiring that customers choosing to accept ACH debits monitor their commercial accounts daily, *see, e.g., id.* ¶¶ 38, 126-29. While, unfortunately, these protections did not prevent the alleged fraud at issue, they are not insignificant. For example, if the alleged fraud in this case had been attempted by a cybercriminal whose fraudulent activity, IP address, or other data matched any data that had been reported to the eFraud Network, the transaction would have been immediately blocked without challenge questions even having been triggered. *See, e.g., id.* ¶ 122. Had Patco monitored its commercial accounts daily, its scrutiny may well have minimized the extent of the loss. The Bank's adoption of these additional security procedures as of May 2009 weighs in favor of a finding that its security procedures as a whole were commercially reasonable.

I am unpersuaded that, in setting the Dollar Amount Rule threshold at $1, the Bank neutralized an otherwise commercially reasonable security procedure system. First, I find it highly significant that Jack Henry *permitted* its bank customers to adjust the Dollar Amount Rule threshold to any level, including as low as $1, having determined that any configuration chosen

by the customer bank would result in the effective operation of its multifactor authentication product. *See id.* ¶¶ 94-96; Defendant's Additional SMF ¶ 19; Plaintiff's Reply SMF ¶ 19.

Second, while Patco (i) adduces evidence that the setting of the Dollar Amount Rule threshold *did* in fact impact security, with RSA warning bank customers to edit decision rules carefully, slowly, and with great caution in part because such rules did play a "major role" in fraud prevention, *see, e.g.*, Plaintiff's Opposing SMF ¶¶ 95-97, and (ii) points out that Ocean Bank itself claims to have adjusted the Dollar Rule Amount threshold to $1 in response to low-dollar amount frauds, *see, e.g.*, Defendant's SMF ¶¶ 104-05, the premise that the adjustment in question materially altered the properties of the Premium Product security system is flawed. As the Bank argues, even if the Dollar Amount Rule had been set at the Jack Henry default of $1,000, or, for that matter, $16,000, Patco still would have been prompted on most of the occasions on which it made ACH transfers to answer challenge questions, providing virtually the same level of opportunity for interception of its answers to challenge questions as when the threshold was set at $1. There is no dispute that, once keylogging malware captures a user's authentication credentials, including the challenge question answers, they are accessible to the cybercriminal.

Beyond this, even crediting Patco's expert's assertions that the infrequent triggering of challenge questions would have effectively prevented or minimized instances of keylogging cybercrime, as the Premium Product system, if configured correctly, was designed to do, *see, e.g.*, Plaintiff's Opposing SMF ¶¶ 95-97, Patco does not say at what level the Bank should have set its Dollar Amount Rule threshold, for what length of time, and whether comparable banks were aware in May 2009 that setting Dollar Amount Rule thresholds at low amounts increased

the opportunity for keylogging malware fraud and were altering the manner in which they set the Dollar Amount Rule threshold accordingly.[134]

It is apparent, in the light of hindsight, that the Bank's security procedures in May 2009 were not optimal. The Bank would have more effectively harnessed the power of its risk-profiling system if it had conducted manual reviews in response to red flag information instead of merely causing the system to trigger challenge questions. Indeed, it commenced manual reviews in the wake of the transactions at issue here. The use of other systems, such as tokens and out-of-band authentication, also would have improved the security of the Bank's system and might have minimized the loss that occurred in May 2009, assuming, as Patco's expert opines, that despite the destruction of evidence on Patco's computers, the loss fairly can be traced to Zeus/Zbot keylogger malware that intercepted Pierce's authentication credentials.

Yet, as of May 2009, only 2 percent of Jack Henry's bank customers had adopted tokens, *see* Defendant's SMF ¶ 167; Plaintiff's Opposing SMF ¶ 167, Ocean Bank had concluded (reasonably, in my view) that Jack Henry's offered version of out-of-band authentication did not offer significantly greater security, *see* Defendant's Opposing SMF ¶ 118, and Jack Henry did not require manual review, *see id*. ¶ 37. Patco says that Ocean Bank could have, and should have, as of May 2009, gone beyond the confines of its Jack Henry product to obtain and implement tokens and better versions of out-of-band authentication, and should have by then implemented manual review. Yet, in so arguing, Patco in effect demands that Ocean Bank have

[134] Patco cites Bank, RSA, and Jack Henry documents in support of the proposition that the Bank understood or should have grasped the security implications of Dollar Amount Rule threshold settings. *See, e.g*., Plaintiff's S/J Motion at 20-21 & n.27; Plaintiff's S/J Opposition at 10-11 & n.8. Yet, inasmuch as appears, these documents did not explicitly address the keylogging malware threat or the manner in which a lower threshold setting might enable such fraud. *See id*. Patco further asserts that Greene, who advises numerous community banks throughout New England on their security procedures, knows of no other banks that have configured their system in the manner that Ocean Bank did. *See* Plaintiff's S/J Opposition at 23. This fact was not set forth in a statement of material facts as required by Local Rule 56, warranting its disregard. In any event, even taking it into consideration, Greene does not indicate that keylogging malware concerns prompted these banks to avoid that configuration.

adopted the best security procedures then available. As the Bank observes, *see* Defendant's S/J Reply at 2-3, that is not the law, *see* Conn. Gen. Stat. Ann. § 42a-4A-203 cmt. 4; 11 M.R.S.A. § 4-1203 cmt. 4; *see also, e.g.*, *Braga Filho v. Interaudi Bank*, No. 03 Civ. 4795(SAS), 2008 WL 1752693, at *4 (S.D.N.Y. Apr. 16, 2008), *aff'd*, 354 Fed. Appx. 381 (2d Cir. 2009) (finding bank's security procedures, consisting of a signed order and confirmatory phone call, together with security measure that did not itself qualify as a "security procedure," a signature comparison, commercially reasonable under Article 4A despite "the absence of other procedural safeguards such as telephone logs, recorded conversations, and passwords").[135]

Summary judgment accordingly should be granted to Ocean Bank, and denied to Patco, on Count I.

B. Counts II-VI

The Bank finally seeks summary judgment as to the remaining counts of Patco's complaint on grounds that (i) each is effectively preempted by Article 4A and, (ii) alternatively, there is no genuine dispute of material fact preventing summary judgment in the Bank's favor on the merits of each. *See* Defendant's S/J Motion at 24-28. Patco disputes that any of its claims are preempted but acknowledges that their fate is tied to that of Count I. *See* Plaintiff's S/J Opposition at 25.

The comment to section 4A-102 explains:

[135] Patco relies, in part, on a quotation from a 1991 law review article by J. Kevin French, an advisor to the Article 4A Drafting Committee, in which French stated: "Requiring security procedures to 'keep up with the times' will foster one of the main goals of the model statute, minimization of losses due to fraudulent payment orders. . . . Courts should be reluctant to find a security procedure commercially reasonable merely because other receiving banks are using similar security procedures. Permitting receiving banks to find 'safety in numbers' would not encourage receiving banks to pursue improvements in security procedure technology and could result in commercial reasonableness being synonymous with the lowest common denominator of security procedures in general use." Plaintiff's S/J Motion at 27-28 (quoting J. Kevin French, *Article 4A's Treatment of Fraudulent Payment Orders – The Customer's Perspective*, 42 Ala. L. Rev. 773, 794-95 (1991)). Ocean Bank's security procedures cannot fairly be described as the "lowest common denominator of security procedures in general use" among comparable banks in May 2009.

> Funds transfers involve competing interests – those of the banks that provide funds transfer services and the commercial and financial organizations that use the services, as well as the public interest. These competing interests were represented in the drafting process and they were thoroughly considered. The rules that emerged represent a careful and delicate balancing of those interests and are intended to be the exclusive means of determining the rights, duties and liabilities of the affected parties in any situation covered by particular provisions of the Article. Consequently, resort to principles of law or equity outside of Article 4A is not appropriate to create rights, duties and liabilities inconsistent with those stated in this Article.

Conn. Gen. Stat. Ann. § 42a-4A-102 cmt.; 11 M.R.S.A. § 4-1102 cmt.

Consistent with this admonition, courts have held common law causes of action preempted when (i) the circumstances giving rise to the common law claims are specifically covered by the provisions of Article 4A or (ii) the common law claims would create rights, duties, or liabilities inconsistent with the provisions of that article. *See, e.g., Travelers Cas. & Surety Co. of Am. v. Bank of Am., N.A.*, No. 09 C 06473, 2010 WL 1325494, at *2 (N.D. Ill. Mar. 30, 2010); *Zengen, Inc. v. Comerica Bank*, 158 P.3d 800, 808 (Cal. 2007). *See also, e.g., Ma v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 597 F.3d 84, 89-90 (2d Cir. 2010) ("For Article 4A purposes, the critical inquiry is whether its provisions protect against the type of underlying injury or misconduct alleged in a claim.").

The Bank correctly analyzes Counts II (negligence), III (breach of contract), and IV (breach of fiduciary duty) as displaced by Article 4A. The gravamen of all three counts is precisely the same as that of Count I: that the Bank failed to employ proper security procedures, as a result of which Patco suffered the loss in question. *Compare* Complaint ¶¶ 49-59 *with id.* ¶¶ 60-73. The Bank accordingly is entitled to summary judgment as to Counts II, III, and IV.

Counts V (unjust enrichment) and VI (conversion) implicate a different transaction: the Bank's alleged improper drawing on Patco's line of credit to cover the alleged fraudulent withdrawals, as a result of which additional interest was assessed on that line of credit. *See id.*

¶¶ 74-82. Hence, these two counts seemingly are not displaced by Article 4A. *See, e.g.*, *Ma*, 597 F.3d at 89 ("Claims that, for example, are not about the mechanics of how a funds transfer was conducted may fall outside of this regime [Article 4A]."); *Schlegel v. Bank of America, N.A.*, 628 S.E.2d 362, 368 (Va. 2006) (while common law claims involving alleged unauthorized payment orders were preempted by Article 4A, common law claims arising from a second transaction, the freezing by the bank of the funds that were the subject of the allegedly unauthorized payment orders, was not preempted). Nonetheless, as Patco itself acknowledges, the viability of these two counts hinges on the success of Count I. *See* Plaintiff's S/J Opposition at 25. If the Bank employed commercially reasonable security procedures, it cannot have been unjustly enriched, or have wrongly converted Patco's funds, when it drew on Patco's line of credit pursuant to the Sweep Agreement to cover the allegedly unauthorized withdrawals. Because I have recommended that the court grant summary judgment in the Bank's favor and against Patco on Count I, I recommend that it also grant summary judgment in the Bank's favor on Counts V and VI.

IV. Conclusion

For the foregoing reasons, I recommend that the court **GRANT** the Bank's motion for summary judgment as to all counts of Patco's complaint and **DENY** Patco's cross-motion for summary judgment as to Count I. This recommended disposition, if adopted, will **MOOT** Patco's and the Bank's motions to exclude expert testimony (Docket Nos. 77 & 64) and the Bank's motion to strike Patco's jury demand (Docket No. 66).

NOTICE

A party may file objections to those specified portions of a magistrate judge's report or proposed findings or recommended decisions entered pursuant to 28 U.S.C. § 636(b)(1)(B) for which de novo review by the district court is sought, together with a supporting memorandum and request for oral argument before the district judge, if any is sought, within fourteen (14)

days after being served with a copy thereof. A responsive memorandum and any request for oral argument before the district judge shall be filed within fourteen (14) days after the filing of the objection.

Failure to file a timely objection shall constitute a waiver of the right to de novo review by the district court and to appeal the district court's order.

Dated this 27th day of May, 2011.

/s/ John H. Rich III
John H. Rich III
United States Magistrate Judge