684 F.3d 197
**(Cite as: 684 F.3d 197)**

H

United States Court of Appeals,
First Circuit.
PATCO CONSTRUCTION COMPANY, INC.,
Plaintiff, Appellant,
v.
PEOPLE'S UNITED BANK, d/b/a Ocean Bank, Defendant, Appellee.

No. 11–2031.
Heard April 5, 2012.
Decided July 3, 2012.

**Background:** Commercial customer filed action in diversity against bank, alleging negligence, breach of contract, breach of fiduciary duty, unjust enrichment, conversion, and that bank's security system was not commercially reasonable and that it had not consented to security procedures, after thieves had electronically stolen hundreds of thousands of dollars from its accounts. The United States District Court for the District of Maine, D. Brock Hornby, J., 2011 WL 3420588, adopted the report and recommendation of John H. Rich, III, United States Magistrate Judge, 2011 WL 2174507, and granted summary judgment for bank. Customer appealed.

**Holdings:** The Court of Appeals, Lynch, Chief Judge, held that:
(1) security procedures employed for Internet banking were not commercially reasonable;
(2) factual issue existed as to what obligations or responsibilities, if any, were imposed on commercial customer; and
(3) Uniform Commercial Code for Funds Transfers, as codified under Maine Law, restrained common law claims, such as breach of contract or breach of fiduciary duty, only to extent that they create rights, duties, and liabilities inconsistent with those statutes.

Affirmed in part, reversed in part, and remanded.

West Headnotes

**[1] Federal Civil Procedure 170A 2470.1**

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)1 In General
170Ak2465 Matters Affecting Right to Judgment
170Ak2470.1 k. Materiality and genuineness of fact issue. Most Cited Cases

On a motion for summary judgment, 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. Fed.Rules Civ.Proc.Rule 56, 28 U.S.C.A.

**[2] Federal Civil Procedure 170A 2470.1**

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)1 In General
170Ak2465 Matters Affecting Right to Judgment
170Ak2470.1 k. Materiality and genuineness of fact issue. Most Cited Cases

On a motion for summary judgment, a fact is material if it has the potential of determining the outcome of the litigation. Fed.Rules Civ.Proc.Rule 56, 28 U.S.C.A.

**[3] Banks and Banking 52 188.5**

52 Banks and Banking
52III Functions and Dealings
52III(F) Exchange, Money, Securities, and Investments
52k188.5 k. Transmission of money or credit in general. Most Cited Cases

Security procedures employed for Internet banking were not commercially reasonable under Uniform Commercial Code for Funds Transfers, as codified under Maine Law, where bank neither monitored transactions, nor provided notice to customers, when it had warning that fraud likely was occurring, before allowing transaction to be completed, and bank asked for security answers for every $1 transaction, which substantially increased risk of fraud, particularly for customers that had frequent, regular, and high dollar transfers, by allowing cyber criminals equipped with keyloggers to have much more frequent opportunity to

capture all information necessary to compromise account. 11 M.R.S.A. §§ 4–1102, 4–1202.

**[4] Federal Civil Procedure 170A 2487**

170A Federal Civil Procedure
170AXVII Judgment
170AXVII(C) Summary Judgment
170AXVII(C)2 Particular Cases
170Ak2487 k. Banks, cases involving. Most Cited Cases

Genuine issue of material fact existed as to what obligations or responsibilities, if any, were imposed on commercial customer, even where bank's Internet banking security system was commercially unreasonable, precluding summary judgment in customer's action against bank, alleging unjust enrichment, conversion, and that bank's security system was not commercially reasonable and that it had not consented to security procedures, after thieves had electronically stolen hundreds of thousands of dollars from its accounts. Fed.Rules Civ.Proc.Rule 56, 28 U.S.C.A.; 11 M.R.S.A. §§ 4–1102, 4–1202.

**[5] Banks and Banking 52 188.5**

52 Banks and Banking
52III Functions and Dealings
52III(F) Exchange, Money, Securities, and Investments
52k188.5 k. Transmission of money or credit in general. Most Cited Cases

Uniform Commercial Code for Funds Transfers, as codified under Maine Law, restrained common law claims, such as breach of contract or breach of fiduciary duty, only to extent that they create rights, duties, and liabilities inconsistent with those statutes. 11 M.R.S.A. § 4–1101 et seq.

***199** Daniel J. Mitchell, with whom Eben M. Albert–Knopp and Bernstein Shur were on brief, for appellant.

Brenda R. Sharton, with whom Don M. Kennedy, Katherine A. Borden, and Goodwin Procter LLP were on brief, for appellee.

Before LYNCH, Chief Judge, LIPEZ and HOWARD, Circuit Judges.

LYNCH, Chief Judge.

Over seven days in May 2009, Ocean Bank, a southern Maine community bank, authorized six apparently fraudulent withdrawals, totaling $588,851.26, from an account held by Patco Construction Company, after the perpetrators correctly supplied Patco's customized answers to security questions. Although the bank's security system flagged each of these transactions as unusually "high-risk" because they were inconsistent with the timing, value, and geographic location of Patco's regular payment orders, the bank's security system did not notify its commercial customers of this information and allowed the payments to go through. Ocean Bank was able to block or recover $243,406.83, leaving a residual loss to Patco of $345,444.43.

Patco brought suit, setting forth six counts against People's United Bank, a regional bank which had acquired Ocean Bank. The suit alleged, inter alia, that the bank should bear the loss because its security system was not commercially reasonable under Article 4A of the Uniform Commercial Code ("UCC"), as codified under Maine Law at Me.Rev.Stat. Ann. tit. 11, § 4–1101 *et seq.*, and that Patco had not consented to the procedures.

On cross-motions for summary judgment,[FN1] the district court held that the bank's security system was commercially reasonable and on that basis entered judgment in favor of the bank on the first count. *Patco Constr. Co. v. People's United Bank*, No. 09–cv–503, 2011 WL 3420588 (D.Me. Aug. 4, 2011). The district court also granted summary judgment in favor of the bank on the remaining counts, holding that they were either dependent on or displaced by the analysis and law underlying the first count. *Id.*

FN1. The parties dispute whether Maine or Connecticut law governs this case. We need not decide this question here as both states have enacted UCC Article 4A, and thus, under either state's laws, the outcome is the same. *Compare* Me.Rev.Stat. Ann. tit. 11, § 4–1101 *et seq.* *with* Conn. Gen.Stat. Ann. § 42a–4A–101 *et seq.* The parties do not identify any difference in the two enactments that would affect our analysis.

We reverse the district court's grant of summary judgment in favor of the bank and affirm its denial of Patco's motion for summary judgment on the first count. In particular, we leave open the question of what, if any, obligations or responsibilities Article 4A imposes on Patco. We also reinstate certain other claims dismissed by the district court, and remand for proceedings consistent with this opinion.

I.

The facts, which are largely undisputed, are as follows. Where the facts remain in dispute, we relate them in the light most favorable to Patco, the non-moving party. *See* *Valley Forge Ins. Co. v. Field*, 670 F.3d 93, 96–97 (1st Cir.2012).

A. *The Parties*

Patco is a small property development and contractor business located in Sanford, Maine. Patco began banking with Ocean Bank in 1985. Ocean Bank was acquired by the Chittenden family of banks, which ***200** was later acquired by People's United Bank, a regional bank based in Bridgeport, Connecticut. People's United Bank operates other local Maine banks such as Maine Bank & Trust, where Patco also had an account in May 2009. Ocean Bank was a division of People's United at the time of the fraudulent withdrawals at issue in this case.

In September 2003, Patco added internet banking-also known as "eBanking"—to its commercial checking account at Ocean Bank. 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. Patco used eBanking primarily to make regular weekly payroll payments. These regular payroll payments had certain repeated characteristics: they were always made on Fridays; they were always initiated from one of the computers housed at Patco's offices in Sanford, Maine; they originated from a single static Internet Protocol ("IP") address; [FN2] and they were accompanied by weekly withdrawals for federal and state tax withholding as well as 401(k) contributions. The highest payroll payment Patco ever made using eBanking was $36,634.74. Until October of 2008, 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.

FN2. "An IP address is the unique address assigned to every machine on the internet. An IP address consists of four numbers separated by dots, e.g., 166.132.78.215." *United States v. Kearney*, 672 F.3d 81, 84 n. 1 (1st Cir.2012) (quoting *United States v. Vázquez–Rivera*, 665 F.3d 351, 354 n. 5 (1st Cir.2011)).

In September 2003, when it added eBanking services, Patco entered into several agreements with Ocean Bank.[FN3] Most significantly, Patco entered into the eBanking for Business Agreement. The 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." The eBanking agreement stated that Ocean Bank did not "assume[ ] any responsibilities" with respect to Patco's use of eBanking, 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. The eBanking agreement also provided that:

> [U]se 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*

FN3. These include the Investment and Line of Credit Sweep Account (Managed Balance Agency Agreement), which authorized Ocean Bank to transfer funds from Patco's account as needed to maintain a target balance in Patco's separate investment account. Patco also signed the Ocean Bank Automated Clearing House Agreement, which provided that Patco was responsible for electronic transfers "purport[ed] to have been transmitted or authorized" by Patco, even if a transfer was not actually authorized by Patco, "provided Bank acted in compliance with the security procedure referred to in Schedule A." Patco asserts that the security procedures provided in Schedule A do not, by their express terms, apply to eBanking transactions such as those here.

> *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.
> ***201** The agreement provided that Patco had to contact the bank immediately upon discovery of an unauthorized transaction.

The bank also reserved the right to modify the terms and conditions of the eBanking agreement at any time, effective upon publication. The bank claims that at some point before May 2009, it modified the eBanking agreement to state:

> 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 agree to notify us of your objection on the same day the debit occurs.

The bank claims that it published this modified eBanking agreement on its website before May 2009. Patco disputes that this agreement was modified and/or published on the bank's website before May 2009, and argues that the modified agreement was therefore not effective as between the parties.

B. *Ocean Bank's Security Measures*

In 2004, Ocean Bank began using Jack Henry & Associates to provide its core online banking platform, known as "NetTeller." Jack Henry provides the NetTeller product to approximately 1,300 of its 1,500 bank customers.

In October 2005, the agencies of the Federal Financial Institutions Examination Council [FN4] ("FFIEC"), responding to increased online banking fraud, issued guidance titled "Authentication in an Internet Banking Environment." *See* Fed. Fin. Insts. Examination Council, Authentication in an Internet Banking Environment (Aug. 8, 2001), *available at* http:// www. ffiec. gov/ pdf/ authentication_ guidance. pdf [hereinafter "FFIEC Guidance"]. The Guidance was intended to aid financial institutions in "evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider." *Id.* at 1. The Guidance provides 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.* at 2.

> FN4. The FFIEC is an interagency body created by statute and charged with "establish[ing] uniform principles and standards and report forms for the examination of financial institutions which shall be applied by the Federal financial institutions regulatory agencies." 12 U.S.C. § 3305(a).

The Guidance explains that existing authentication methodologies involve three basic "factors": (1) something the user knows (e.g., password, personal identification number); (2) something the user has (e.g., ATM card, smart card); and (3) something the user is (e.g., biometric characteristic, such as a fingerprint). *Id.* at 3. 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 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.* The Guidance also states:

> The agencies consider single-factor authentication, as the only control mechanism,***202** 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.

Following publication of the FFIEC Guidance, Ocean Bank worked with Jack Henry to conduct a risk

assessment and institute appropriate authentication protocols to comply with the Guidance. The bank determined that its eBanking product was a "high risk" system that required enhanced security, and in particular, multifactor authentication.

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 the FFIEC Guidance. Through collaboration with RSA/Cyota, Jack Henry made two multifactor authentication products available to its customers to meet the FFIEC Guidance: the "Basic" package and the "Premium" package.

Ocean Bank selected the Jack Henry "Premium" package, which it implemented by January 2007. The system, as implemented by Ocean Bank, had six key features:

1. *User IDs and Passwords:* The system required each authorized Patco employee to use both a company ID and password and a user-specific ID and password to access online banking.

2. *Invisible Device Authentication:* The system placed a "device cookie" onto customers' computers to identify particular computers used to access online banking. The device cookie would be used to help establish a secure communication session with the NetTeller environment and to contribute to the component risk score. Whenever the cookie was changed or was new, that impacted the risk score and potentially triggered challenge questions.

3. *Risk Profiling:* The system entailed the building of a risk profile for each customer by RSA/Cyota based on a number of different factors, including the location from which a user logged in, when/how often a user logged in, what a user did while on the system, and the size, type, and frequency of payment orders normally issued by the customer to the bank. The Premium Product noted the IP address that the customer typically used to log into online banking and added it to the customer profile.

RSA/Cyota's adaptive monitoring provided a risk score to the bank for every log-in attempt and transaction based on a multitude of data, including but not limited to IP address, device cookie ID, Geo location, and transaction activity. If a user's transaction differed from its normal profile, RSA/Cyota reported to the bank an elevated risk score for that transaction. RSA/Cyota considered transactions generating risk scores in excess of 750, on a scale from 0 to 1,000, to be high-risk transactions. "Challenge questions," described below, were prompted any time the risk score for a transaction exceeded 750.

4. *Challenge Questions:* The system required users, during initial log-in, to select three challenge questions and responses. The challenge questions might be prompted for various reasons. For example, if the risk score associated with a particular transaction exceeded 750, the ***203** challenge questions would be triggered. If the challenge question responses entered by the user did not match the ones originally provided, the customer would receive an error message. If the customer was unable to answer the challenge questions in three attempts, the customer was blocked from online banking and would be required to contact the bank.

5. *Dollar Amount Rule:* The system permitted financial institutions to set a dollar threshold amount above which a transaction would automatically trigger the challenge questions even if the user ID, password, and device cookie were all valid. In August 2007, Ocean Bank set the dollar amount rule to $100,000. On June 6, 2008, Ocean Bank lowered the dollar amount rule from $100,000 to $1. After the Bank lowered the threshold to $1, Patco was prompted to answer challenge questions every time it initiated a transaction. In May 2009, when the fraud at issue in this case occurred, the dollar amount rule threshold remained at $1.

6. *Subscription to the eFraud Network:* The Jack Henry Premium Product 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. The eFraud Network allowed financial institutions to report IP addresses or other discrete identifying characteristics identified with instances of fraud. An attempt to access a customer's NetTeller account initiated by someone with that characteristic would then be automatically blocked. The individual would not even be prompted for challenge questions.

Ocean Bank asserts that on December 1, 2006, as it began to implement the Jack Henry system, it also began to offer the option of e-mail alerts to its eBanking customers. If the customer chose to receive such alerts, the bank would send the customer e-mails regarding incoming/outgoing transactions, changes to the customer's balance, the clearing of checks, and/or alerts on certain customer-specified dates. Patco claims it did not receive notice that e-mail alerts were available and this is a disputed issue of fact. It appears that notice of the availability of e-mail alerts was not readily visible. To set up alerts through the eBanking system, a user would have to first click the "Preferences" tab on the eBanking webpage, then click on a second tab labeled "Alerts," and then follow several additional steps to activate individual alerts. Patco claims it never saw anything on the website indicating that e-mail alerts were available, and it therefore never set up e-mail alerts.

C. *Security Measures Available Which Ocean Bank Chose Not to Implement*

There were several additional security measures that were available to Ocean Bank but that the bank chose not to implement:

1. *Out–of–Band Authentication:* Jack Henry offered Ocean Bank a version of the NetTeller system that included an out-of-band authentication option. Out-of-band authentication "generally refers to additional steps or actions taken beyond the technology boundaries of a typical transaction." *Id.* at 3 n.5. Examples of out-of-band authentication include notification to the customer, callback (voice) verification, e-mail approval from the customer, and cell phone based challenge/response processes. The FFIEC Guidance identifies out-of-band authentication as a useful method of risk mitigation. *See id.* at 11–12.

2. *User–Selected Picture:* Ocean Bank's security procedures did not include the user-selected picture function that was ***204** available through Jack Henry's Premium option. Ocean Bank states that it did not utilize the user-selected picture function because it already utilized other anti-phishing [FN5] controls.

> FN5. Phishing involves an attempt to acquire information such as usernames, passwords, or financial data by a perpetrator masquerading as a legitimate enterprise. Typically, the perpetrator will provide an e-mail or link that directs the victim to enter or update personal information at a phony website that mimics an established, legitimate website which the victim either has used before or perceives to be a safe place to enter information.

3. *Tokens:* Tokens are physical devices (something the person has), such as a USB token device, a smart card, or a password-generating token. The FFIEC Guidance identifies tokens as a useful part of a multifactor authentication scheme. *See id.* at 8. Tokens were not available from Jack Henry when Ocean Bank implemented its system in 2007, but were readily available to financial institutions at that time through other sources. Although People's United Bank has used tokens since at least January of 2008, Ocean Bank did not do so until after the fraud in this case occurred.

4. *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 that generated high risk scores. 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. The bank also had the ability to call a customer if it detected fraudulent activity, but did not do so. The bank began conducting manual reviews of high-risk transactions in late 2009, after the fraud in this case occurred. Since then, the bank has instituted a policy of calling the customer in the case of uncharacteristic transactions to inquire if the customer did indeed initiate the transaction.

D. *The Fraudulent Transfers*

Beginning on May 7, 2009, a series of withdrawals were made on Patco's account over the course of several days.

On May 7, unknown third parties initiated a $56,594 ACH withdrawal from Patco's account. The perpetrators supplied the proper credentials of one of Patco's employees, including her ID, password, and answers to her challenge questions. The payment on this withdrawal was directed to go to the accounts of numerous individuals, none of whom had previously been sent money by Patco. The perpetrators logged in

from a device unrecognized by Ocean Bank's system, and from an IP address that Patco had never before used. The risk-scoring engine generated a risk score of 790 for the transaction, a significant departure from Patco's usual risk scores, which generally ranged from 10 to 214. There is no evidence that Patco's risk scores prior to the fraudulent transfers in this case ever exceeded 214. The risk-scoring engine reported the following contributors to the risk score for that transaction: (1) "Very high risk non-authenticated device"; (2) "High risk transaction amount"; (3) "IP anomaly"; and (4) "Risk score distributor per cookie age." 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." Despite this high risk score, Patco was not notified. Moreover, it appears no one at the bank monitored these high-risk transactions. Bank personnel did not manually review the May 7, 2009 transaction. The bank batched and ***205** processed the transaction as usual, and it was paid the next day.

The activities of May 7 having successfully resulted in payment, on Friday, May 8, 2009, unknown third parties again successfully initiated an ACH payment order from Patco's account, this time for $115,620.26. As before, the perpetrators wired money to multiple individual accounts to which Patco had never before sent funds. The perpetrators again used a device that was not recognized by Ocean Bank's system. The payment order originated from the same IP address as the day before. The transaction was larger by several magnitudes than any ACH transfer Patco had ever made to third parties. Despite these unusual characteristics, the bank again took no steps to notify Patco and batched and processed the transaction as usual, which was paid by the bank on Monday, May 11, 2009.

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. Like the prior fraudulent transactions, these transactions were uncharacteristic in that they sent money to numerous individuals to whom Patco had never before sent funds, were for greater amounts than Patco's ordinary third-party transactions, were sent from computers that were not recognized by Ocean Bank's system, and originated from IP addresses that were not recognized as valid IP addresses of Patco. As a result of these unusual characteristics, the transactions continued to generate higher than normal risk scores. The May 11 transaction generated a risk score of 720, the May 12 transaction triggered a risk score of 563, and the transaction on May 13 generated a risk score of 785. The Bank did not manually review any of these transactions to determine their legitimacy or notify Patco.

Portions of the transfers, beginning with the first transfer initiated on May 7, 2009, were automatically returned to the bank because certain of the account numbers to which the money was slated to be transferred were invalid. As a result, the bank sent limited "return" notices to the home of Mark Patterson, one of Patco's principals, via U.S. mail. Patterson received the first such notice after work on the evening of May 13, six days after the allegedly fraudulent withdrawals began.

The next morning, on May 14, 2009, Patco called the bank to inform it that Patco had not authorized the transactions. Also on the morning of May 14, another alleged fraudulent transaction was initiated from Patco's account in the amount of $111,963. Despite the information from Patco, the bank initially processed this payment order on May 15, 2009. However, because of the alert from Patco of the ongoing fraud, the bank then took steps to block completion of a portion of this transaction and recovered a portion of the transferred funds shortly thereafter.

At the end of the string of thefts, the amount of money fraudulently withdrawn from Patco's account totaled $588,851.26, of which $243,406.83 was automatically returned or blocked and recovered.

According to Ocean Bank, on May 14, 2009, immediately after the allegedly fraudulent withdrawals occurred, the bank gave instructions to Patco. It instructed Patco to disconnect the computers it used for electronic banking from its network; to stop using these computers for work purposes; to leave the computers turned on; and to 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. Ocean Bank claims, and Patco disputes, that Patco did not isolate its computers or forensically preserve the hard ***206** drives; and that Patco employees continued to use their computers during the week following the alleged

fraud. In another dispute of fact, Patco states that Ocean Bank recommended only that Patco check its system for a security breach using a third-party forensic professional, which Patco did.

Shortly after the fraudulent transfers, Patco hired an IT consultant, who ran anti-malware scans on the computers. A remnant of a Zeus/Zbot malware was found. However, the Zeus/Zbot malware, which contained the encryption key for the Zeus/Zbot configuration file, was quarantined and then deleted by the anti-malware scan. Without the encryption key, it is impossible to decrypt the configuration file and identify what information, if any, the Zeus/Zbot malware would have captured, if in fact it was of a type that would have intercepted authentication credentials.

II.

On September 18, 2009, Patco filed suit against People's United in Maine Superior Court, York County. The complaint included six counts: (I) liability under Article 4A of the Uniform Commercial Code ("UCC"); (II) negligence; (III) breach of contract; (IV) breach of fiduciary duty; (V) unjust enrichment; and (VI) conversion. On October 9, 2009, People's United removed the case to the United States District Court for the District of Maine.

On August 27, 2010, Patco moved for summary judgment on Count I, its claim under Article 4A of the UCC. That same day, the bank moved for summary judgment on all six counts. On May 27, 2011, the magistrate judge issued a recommended decision on the cross-motions for summary judgment. *Patco Constr. Co. v. People's United Bank*, No. 09–cv–503, 2011 WL 2174507 (D.Me. May 27, 2011). The magistrate judge determined both that the bank's security procedures were commercially reasonable, *id.* at *32–34, and that Patco had agreed to those procedures, *id.* at *24–25. Therefore, the magistrate concluded, Patco—not the bank—bore the loss of the fraudulent transfers. *Id.* at *34. The magistrate also determined that Counts II–IV of Patco's complaint were displaced by the provisions of Article 4A, and that Counts V and VI failed along with Count I because the bank could not have been unjustly enriched, or have wrongly converted Patco's funds, if it employed commercially reasonable security procedures. *Id.* at *34–35. Accordingly, the magistrate recommended that the district court grant the bank's motion for summary judgment and deny that of Patco. *Id.* at *35.

Patco objected to the recommended decision on June 13, 2011, and People's United responded to Patco's objection on June 27, 2011. On August 4, 2011, the district court adopted the magistrate's recommendation in full. It granted People's United's motion for summary judgment, denied Patco's motion for summary judgment, and found the parties' outstanding motions to be moot. On September 6, 2011, Patco appealed.

III.

We review orders granting or denying summary judgment de novo. *Certain Interested Underwriters at Lloyd's, London v. Stolberg*, 680 F.3d 61, 65 (1st Cir.2012). In doing so, we consider the record and all reasonable inferences in the light most favorable to the non-moving party. *Id.*

[1][2] We affirm only if there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law. *Id.* "A dispute is genuine if the evidence about the fact is such that a reasonable jury could resolve the point in ***207** 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 *Maymí v. P.R. Ports Auth.*, 515 F.3d 20, 25 (1st Cir.2008)).

A. *Article 4A of the UCC*

[3] The claim under Count I is governed by Article 4A of the UCC, which was meant to govern the rights, duties, and liabilities of banks and their commercial customers with respect to electronic funds transfers. *See* Me.Rev.Stat. Ann. tit. 11, § 4–1102 cmt. Article 4A was enacted in toto by Maine in 1991, well before the transfers at issue in this case.[FN6] *Id.* § 4–1101.

> FN6. In its enactment of Article 4A, the Maine legislature provided that while "the text of that uniform act has been changed to conform to Maine statutory conventions[, ... u]nless otherwise noted in a Maine comment, the changes are technical in nature and it is the intent of the Legislature that this Act be interpreted as substantively the same as the uniform act." 1992 Me. Legis. Serv. ch. 812,

§ 3.

Article 4A was developed to address wholesale wire transfers and commercial ACH transfers, generally between businesses and their financial institutions. [FN7] *Id.* § 4–1102 cmt. Before Article 4A was drafted, "there was no comprehensive body of law—statutory or judicial—that defined the juridical nature of a [commercial] funds transfer or the rights and obligations flowing from payment orders." *Id.* Instead, judges relied on general principles of common law, sought guidance from other provisions of the UCC, or analogized to laws applicable to other payment methods. *Id.* The drafters of Article 4A sought to deliver clarity to this area of law by "us[ing] precise and detailed rules to assign responsibility, define behavioral norms, allocate risks and establish limits on liability" in order to allow parties to predict and insure against risk with greater certainty, given the very large amounts of money involved in commercial funds transfers. *Id.*

> FN7. By contrast, *consumer* payments that are made electronically, such as through direct wiring or the use of a debit card, are covered by a separate federal statute, the Electronic Fund Transfer Act (EFTA), 15 U.S.C. § 1693 *et seq.* Article 4A does not apply to any funds transfer that is covered by the EFTA; the two are mutually exclusive. Me.Rev.Stat. Ann. tit. 11, § 4–1108 & cmt. The drafters of Article 4A felt that a separate framework, apart from the more consumer-focused EFTA, was needed to cover electronic transfers between commercial institutions because of the sheer volume and magnitude of such transfers. *Id.* Art. 4–A, Refs. & Annots. cmt. At the time of Article 4A's drafting, the volume of payments by non-consumer wire transfer exceeded well over one trillion dollars per day and the dollar volume of payments made by wire transfer far exceeded the dollar volume of payments made by other means. *Id.*

Importantly, the drafters also sought to clarify the interaction between the new provisions of Article 4A and existing remedies under the common law:

> 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***208** 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.

*Id.* The drafters "intended that Article 4A would be supplemented, enhanced, and in some places, superceded by other bodies of law ... [T]he Article is intended to synergize with other legal doctrines," so long as those doctrines are not inconsistent with the rights, duties, and liabilities established in Article 4A. *Regions Bank v. Provident Bank, Inc.*, 345 F.3d 1267, 1275 (11th Cir.2003) (omission in original) (quoting Baxter & Bhala, *The Interrelationship of Article 4A with Other Law*, 45 Bus. Law. 1485, 1485 (1990)) (internal quotation mark omitted). Article 4A further provides that, in general, the parties may not vary by agreement any rights and obligations arising under Article 4A. *See* Me.Rev.Stat. Ann. tit. 11, § 4–1202(6).

Under Article 4A, a bank receiving a payment order ordinarily bears the risk of loss of any unauthorized funds transfer. *Id.* § 4–1204. The bank may shift the risk of loss to the customer in one of two ways, one of which involves the commercial reasonableness of security procedures and one of which does not. First, the bank may show that the "payment order received ... is the authorized order of the person identified as sender if that person authorized the order or is otherwise bound by it under the law of agency." *Id.* § 4–1202(1). But, as the Article 4A commentary explains, "[i]n a very large percentage of cases covered by Article 4A, ... [c]ommon law concepts of authority of agent to bind principal are not helpful" because the payment order is transmitted electronically and the bank "may be required to act on the basis of a message that appears on a computer screen." *Id.* § 4–1203 cmt. 1.

If the sender of the payment order had no authority to act for the customer, and there are no additional

facts on which estoppel might be found, the "Customer is not liable to pay the order and [the] Bank takes the loss." *Id.* cmt. 2. In such cases, "these legal principles [of agency] give the receiving bank very little protection.... The only remedy of [the] Bank is to seek recovery from the person who received payment as beneficiary of the fraudulent order." *Id.* cmts. 1, 2.

Accordingly, the drafters provided a second way by which a bank may shift the risk of loss and protect itself whether or not the payment order is authorized. This, in turn, has several components:

> 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:
>
> (a) The security procedure is a commercially reasonable method of providing security against unauthorized payment orders; and
>
> (b) 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. The bank is not required to follow an instruction that violates a written agreement with the customer or notice of which is not received at a time and in a manner affording the bank a reasonable opportunity to act on it before the payment order is accepted.

*Id.* § 4–1202(2).

In turn, Article 4A defines a security procedure as:

> ***209** [A] procedure established by agreement of a customer and a receiving bank for the purpose of: (1) Verifying that a payment order or communication amending or cancelling a payment order is that of the customer; or (2) Detecting error in the transmission or the content of the payment order or communication.

*Id.* § 4–1201. One question raised in this appeal is the scope of any agreement reached.

The UCC explains that the "[c]ommercial reasonableness of a security procedure is a question of law" to be determined by the court. *Id.* § 4–1202(3). There are two ways by which a security procedure may be shown to be commercially reasonable. First is by reference to:

> [T]he wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type and 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.

*Id.* § 4–1202(3). The Article is explicit that "[t]he 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...." *Id.* § 4–1203 cmt. 4. The UCC explains that "[t]he 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." *Id.* cmt. 3.

Secondly, the Article creates a presumption of reasonableness under certain circumstances, not applicable here. A security procedure is deemed to be commercially reasonable if:

> (a) 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
>
> (b) 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.

*Id.* § 4–1202(3). Of course, if the security procedure offered by the bank was not commercially reasonable, then the provision does not apply. *Id.* § 4–1203 cmt. 4.

If the bank shows both that its security procedure was commercially reasonable and that it accepted the payment order "in good faith and in compliance with the security procedure," the payment order is effective as an authorized order of the customer. *Id.* §§ 4–1202(2)(b), 4–1203(1). In such a case, the bank may, "[b]y express written agreement, ... limit the extent to which it is entitled to enforce or retain payment of the payment order." *Id.* § 4–1203(1)(a).

Once the bank has shown commercial reasonableness, the customer may shift the risk of loss back to the bank if the customer proves that the order was not "caused, either directly or indirectly, by a person":

> (i) Entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure or who obtained access to transmitting facilities of the customer; or
>
> (ii) Who obtained from a source controlled by the customer and without authority of the receiving bank information facilitating breach of the security procedure, regardless of how the information was obtained or whether the customer was at fault. Information includes any ***210** access device, computer software or the like.

*Id.* § 4–1203(1)(b). As the commentary explains, this section of the UCC places a burden on the customer, when the security procedure is commercially reasonable, "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." *Id.* § 4–1203 cmt. 3.

If the bank does not make its showing of commercial reasonableness, then the analysis goes back to the question of agency under § 4–1202(a), described above. If the court determines, under any of these provisions, that the bank bears the risk of loss, "the bank shall refund any payment of the payment order received from the customer to the extent the bank is not entitled to enforce payment and shall pay interest on the refundable amount calculated from the date the bank received payment to the date of the refund." *Id.* § 4–1204(1).

B. *Ocean Bank's Motion for Summary Judgment*

Ocean Bank argues that because Patco agreed to the security system in use, and because the security system was commercially reasonable, it is entitled to summary judgment.

Patco counters that the bank's security system was not commercially reasonable, that it did not agree to all of the procedures, and that the bank did not comply with its own procedures.

As to commercial reasonableness, Patco argues the bank's decision to lower the dollar amount rule to $1 increased the risk of compromised security, and that the bank's failure in light of this increased risk to monitor and immediately notify customers of abnormal transactions which met high risk criteria was not commercially reasonable. Patco also argues that it was not offered and it did not decline an e-mail notice system for transactions.

Essentially, Patco argues that when Ocean Bank decided in June of 2008 to trigger challenge questions for any transaction over $1, the bank increased the frequency with which a user was required to enter the answers to his or her challenge questions. Indeed, at a $1 threshold, the frequency as to Patco became 100%, covering every transaction. For customers like Patco who made regular ACH transfers, the risks were even greater than for customers who rarely made such transfers. This, in turn, also increased the risk that such answers would be compromised by keyloggers [FN8] or other malware that would capture that information for unauthorized uses. By thus increasing the risk of fraud through unauthorized use of compromised security answers, Patco argues, Ocean Bank's security system failed to be commercially reasonable because it did not incorporate additional security measures, at the very least monitoring of high risk score transactions, use of e-mail alerts and inquiries, or other immediate notice to customers of high-risk transactions.

> FN8. 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. In this way, the keylogger is able to capture a user's authentication credentials, which the keylogger then transmits to a cyber thief.

In our view, Ocean Bank did substantially increase the risk of fraud by asking for security answers for every $1 transaction, particularly for customers like Patco which had frequent, regular, and high dollar ***211** transfers. Then, when it had warning that such fraud was likely occurring in a given transaction, Ocean Bank neither monitored that transaction nor provided notice to customers before allowing the transaction to be completed. Because it had the capacity to do all of those things, yet failed to do so, we cannot conclude that its security system was commercially reasonable. We emphasize that it was these collective failures taken as a whole, rather than any single failure, which rendered Ocean Bank's security system commercially unreasonable.

The Jack Henry Premium Product was designed to harness the power of the risk-scoring system and included a device identification system to trigger an additional layer of authentication—challenge questions—whenever the bank's system detected unusual or suspicious transactions. In May of 2009, bank personnel did not monitor the risk-scoring reports, nor did the bank conduct any other regular review of transactions that generated high risk scores. Thus, the only result of a high risk score or an unidentified device was that a customer would be prompted to answer his or her challenge questions.

When Ocean Bank lowered the dollar amount rule from $100,000 to $1, it essentially deprived the complex Jack Henry risk-scoring system of its core functionality. The $1 dollar amount rule guaranteed that challenge questions would be triggered on every transaction unless caught by a separate eFraud network which depended on the use of known fraudulent IP addresses. The eFraud network was of no use if the address and like information were not already known to law enforcement. Accordingly, cyber criminals equipped with keyloggers had the much more frequent opportunity to capture all information necessary to compromise an account every time the customer initiated an ACH transaction. In Patco's case, ACH transactions were initiated at least weekly, and often several times per week. In the event a customer's computer became infected with a keylogger, it was likely that the customer would be prompted to answer its challenge questions before the malware was discovered and removed from the customer's computer.

Patco's argument is supported both by evidence and by common sense. Patco's expert testified that at the times in question, keylogging malware was a persistent problem throughout the financial industry. It was foreseeable, against this background, that triggering the use of the same challenge questions for high-risk transactions as were used for ordinary transactions, was ineffective as a stand-alone backstop to password/ID entry. Indeed, it was well known that setting challenge questions to be asked on every transaction greatly increases the risk that a fraudster equipped with a keylogger would be able to access the answers to a customer's challenge questions because it increases the frequency with which such information is entered through a user's keyboard.

As early as 2005, RSA/Cyota cautioned against the regular and frequent use of challenge questions as a stand-alone backstop to the exclusion of further controls, stating that challenge questions were "quicker and simpler to adopt" but were "less secure," and should be used only "in the short term, as the first phase of a full project." According to RSA/Cyota, challenge questions should be triggered only selectively, when unusual or suspicious activity is detected, so that they are less likely to be asked after a keylogger is installed on a customer's computer and before it can be removed. When asked frequently, they should not be used as the only line of defense beyond a password/ID, ***212** since a password/ID and answers to challenge questions could all be simultaneously captured by a keylogger.

Ocean Bank's decision to set the dollar amount rule at $1 for all of its customers also ignored Article 4A's mandate that security procedures take into account "the circumstances of the customer" known to the bank. *Id.* § 4–1202(3). Article 4A directs banks to consider such circumstances as "the size, type and frequency of payment orders normally issued by the customer to the bank." *Id.* In Patco's case, these characteristics were regular and predictable. Patco used eBanking primarily to make payroll payments to employees. These payments were made weekly, generally on Fridays; they originated from a single static IP address; and they were always made from the same set of computers at Patco's offices in Sanford, Maine. The highest such payment Patco ever made was $36,634.74, well below the former $100,000 threshold. The bank does not assert that it ever offered to adjust the threshold amount for particular customers.

Instead, the bank adopted a "one-size-fits-all" dollar amount rule of $1 for its customers.

Ocean Bank argues that it did take Patco's circumstances into account by building a risk profile based on Patco's eBanking habits, such that the security system could compare the characteristics of each transaction against those in Patco's profile.[FN9] This argument misses the mark because, in fact, the risk profile information played no role. It triggered no additional authentication requirements, and the bank did nothing with the information generated by comparing the fraudulent transactions against Patco's profile.

> FN9. The bank also argues that it took Patco's circumstances into account by setting Patco's **ACH** withdrawal limit based on its specific needs. As the district court correctly noted, however, **ACH** limits do not constitute a "**security procedure**" under Article 4A and thus have no bearing on the commercial reasonableness analysis. *Patco Constr. Co. v. People's United Bank*, No. 09–cv–503, 2011 WL 2174507, at *28 n. 131 (D.Me. May 27, 2011).

Ocean Bank also argues that it was commercially reasonable for it to universally lower the dollar amount rule to $1 in order to target low-dollar fraud. Whether or not that is true for certain customers, it is beside the point. Here, the increase in risk to the consumer who engaged in regular high dollar transfers, such as Patco, was sufficiently serious to require a corollary increase in security measures for a security system to remain commercially reasonable. The bank's generic "one-size-fits-all" approach to customers violates Article 4A's instruction to take the customer's circumstances into account. Further, the reduction of the dollar amount rule to $1 was for commercial customers, who are quite unlikely to have transfers of less than $1.

Ocean Bank introduced no additional security measures in tandem with its decision to lower the dollar amount rule, despite the fact that several such security measures were not uncommon in the industry and were relatively easy to implement. Patco's expert testified that all of her other banking clients using the same Jack Henry Premium Product employed manual reviews or some other additional security measure to protect against the type of fraud that occurred in this case.

For example, by May 2009, internet banking security had largely moved to hardware-based tokens and other means of generating "one-time" passwords.[FN10] As of ***213** then, People's United Bank (which had acquired Ocean Bank), several national banks, and many New England community banks were using tokens for commercial accounts. Of those banks that did not use tokens in May 2009, New England community banks commonly used some form of manual review or customer verification to authenticate uncharacteristic or suspicious transactions. Such security procedures self-evidently would not have been difficult to implement.[FN11]

> FN10. Although tokens can be compromised, bypassing them requires greater sophistication than is needed to obtain challenge questions. The perpetrator must use the information within seconds of acquiring it, before the system generates a new password to replace the old. The answers to challenge questions, by contrast, may be used at the perpetrator's leisure, particularly when, as was the case at Ocean Bank, the answers are static. 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.

> FN11. Indeed, shortly after the fraud in this case occurred, Ocean Bank began conducting manual reviews of suspect transactions. Now, transactions that generate high risk scores are personally reviewed by Ocean Bank personnel to determine their legitimacy.

This failure to implement additional procedures was especially unreasonable in light of the bank's knowledge of ongoing fraud. As early as 2008, Ocean Bank had received notification of substantial increases in internet fraud involving keylogging malware. By May 2009, Ocean Bank had itself experienced at least two incidents of fraud on the bank's system which it attributed to either keylogging malware or internal fraud. In both instances, the perpetrators had acquired

and successfully applied the customer's passwords, IDs, and answers to challenge questions.

Thus, by May 2009, when the fraud in this case occurred, it was commercially unreasonable for Ocean Bank's security system to trigger nothing more than what was triggered in the event of a perfectly ordinary transaction in response to the high risk scores that were generated by the withdrawals from Patco's account. The payment orders at issue were entirely uncharacteristic of Patco's ordinary transactions: they were directed to accounts to which Patco had never before transferred money; they originated from computers Patco had never before used; they originated from an IP address that Patco had never before used; and they specified payment amounts significantly higher than the payments Patco ordinarily made to third parties. As a result, the security system flagged these transactions as uncharacteristic, highly suspicious, and potentially fraudulent from a "very high risk non-authenticated device." The transactions generated unprecedentedly high risk scores ranging from 563 to 790, well above Patco's regular risk scores which ranged from 10 to 214.

These collective failures, taken as a whole, rendered Ocean Bank's security procedures commercially unreasonable. We reverse the district court's grant of summary judgment as to Count I.

That does not, however, end the matter, even as to Count I. The issues briefed to us on appeal have largely involved commercial reasonableness. Our conclusion that the security procedures were not commercially reasonable does not end the analysis of the Article 4A issues. Our conclusion as to Count I and commercial reasonableness does, though, also lead us to vacate the district court's grant of summary judgment on the two claims—Count V (unjust enrichment) and Count VI (conversion)—which the district court considered to be dependent on the success of Count I.

C. *Patco's Motion for Summary Judgment*

[4] We affirm the district court's decision to deny Patco's motion for summary ***214** judgment. There remain several genuine and disputed issues of fact which may be material to the question of whether Patco has satisfied its obligations and responsibilities under Article 4A, or at least to the question of damages. The district court did not reach, and the parties have not briefed, the question of what, if any, obligations or responsibilities Article 4A imposes on a commercial customer even where a bank's security system is commercially unreasonable. We leave these questions open on remand so that the district court may, after briefing, assess whether such obligations exist, either for liability purposes or for mitigation of damages.

As to the genuine and disputed issues of fact, the parties dispute the facts surrounding Patco's lack of e-mail alerts. Patco alleges that it requested e-mail alerts from the bank, but that the bank ignored these requests and never notified Patco when e-mail alerts became available to bank customers. The bank counters with its own allegation that it sent out a general e-mail to customers that it would make e-mail alerts available. Patco states that it received no such e-mail, and that instead, a customer would have had to follow a complicated series of steps to find an "Alerts" tab on the bank's website in order to learn that such e-mail alerts had become available. Moreover, Patco alleges that its account was not even set up with an "Alerts" tab; that the account only features a "Preferences" tab. While one of Patco's employees did successfully navigate to the "Preferences" tab, she alleges she never saw an "Alerts" tab. Additionally, neither party has submitted into the record an example of such an e-mail alert or specified when such an e-mail alert would have been sent, such that it is unclear what Patco would have learned from such an e-mail alert and whether and when such an e-mail would have placed Patco on notice of the fraudulent transfer.

The parties also disagree as to whether the fraud in this case was caused by malware and keylogging in the first place, or whether Patco shares some responsibility. Ocean Bank argues that because Patco irreparably altered the evidence on its hard drives by using and scanning its computers before making forensic copies, it is unclear whether keylogging malware existed on Patco's computers and enabled the alleged fraud. These disputed issues of fact may be material.

Article 4A does not appear to be a one-way street. Commercial customers have obligations and responsibilities as well, under at least § 4–1204. *See* Me.Rev.Stat. Ann. tit. 11, § 4–1204; *but see id.* § 4–1102 cmt. ("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."). Section 4–1204, entitled "Refund of

payment and duty of customer to report with respect to unauthorized payment order," provides:

> The customer is not entitled to interest from the bank on the amount to be refunded if the customer fails to exercise ordinary care to determine that the order was not authorized by the customer and to notify the bank of the relevant facts within a reasonable time not exceeding 90 days after the date the customer received notification from the bank that the order was accepted or that the customer's account was debited with respect to the order.

*Id.* § 4–1204(1).[FN12] It is unclear, however, what, if any, obligations a commercial customer***215** has when a bank's security system is found to be commercially unreasonable.

> FN12. The commentary describes this burden on the customer as a duty of ordinary care which is designed to encourage the customer to promptly notify the bank about any instances of fraud so that the bank can minimize its losses. Me.Rev.Stat. Ann. tit 11, § 4–1204 cmt. 2. The commentary clarifies that a breach of this duty results only in a loss of the interest on the refund payable by the bank, but not a loss of the refund itself. *Id.*

In short, we leave open for the parties to brief on remand the question of what, if any, obligations or responsibilities are imposed on a commercial customer under Article 4A even where a bank's security system is commercially unreasonable. The record requires further development on these issues, precluding summary judgment at this stage.

D. *Dismissal of Counts II–IV*

[5] The district court concluded that Article 4A "preempts" [FN13] Patco's remaining common law claims: Count II (negligence), Count III (breach of contract), and Count IV (breach of fiduciary duty). The district court based its analysis on the commentary to § 4–1102, which provides:

> FN13. This use of the term has nothing to do with the standard legal use of "preemption," which involves the question of whether federal law precludes a state from regulating on the same topic. *See, e.g.*, *Kurns v. R.R. Friction Prods. Corp.*, —— U.S. ——, 132 S.Ct. 1261, 1265–66, ——L.Ed.2d —— (2012). We prefer different terminology.

> 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.
> *Id.* § 4–1102 cmt.

This language does not, on its face, displace Patco's Count III for breach of contract or Count IV for breach of fiduciary duty.[FN14] We adopt the test, as set forth in the commentary, that Article 4A embodies an intent to restrain common law claims only to the extent that they create rights, duties, and liabilities *inconsistent* with Article 4A. *See Ma v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 597 F.3d 84, 89 (2d Cir.2010); *Regions Bank*, 345 F.3d at 1275.

> FN14. We do not address whether Patco otherwise states a claim for breach of fiduciary duty under Maine Law, *see, e.g.*, *Stewart v. Machias Sav. Bank*, 762 A.2d 44, 46 & n. 1 (Me.2000), or for that matter, breach of contract, *see, e.g.*, *Seashore Performing Arts Ctr., Inc. v. Town of Old Orchard Beach*, 676 A.2d 482, 484 (Me.1996).

The common law claims of breach of contract and breach of fiduciary duty are not inherently inconsistent with Patco's Article 4A claim. At least in theory, there could be, either by contract or through assumption of fiduciary duties,[FN15] higher standards which are imposed on the bank. Indeed, courts have held that plaintiffs may turn to common law remedies to seek redress for an alleged harm arising from a funds transfer where Article 4A does not ***216** protect against the underlying injury or misconduct alleged. *See, e.g.*, *Ma*, 597 F.3d at 89–90; *Regions Bank*, 345 F.3d at 1275; *see also* White & Summers, Uniform

Commercial Code §§ 1–2, at 132 (1993 pocket part) ("With the adoption of Article 4A, electronic funds transactions are governed not only by Article 4A, but also common law...."). We vacate the dismissal and leave the issue of these two causes of action open on remand to be considered anew.

> FN15. We disagree with the district court's conclusion that inconsistency is demonstrated merely because "[t]he 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." *Patco Constr. Co.*, 2011 WL 2174507, at *35.

The closer question is whether Article 4A, on the facts of this case, [FN16] displaces the claim for negligence. That is, are the negligence claims inconsistent with the duties and liability limits set forth in Article 4A. We think they are, inasmuch as the standard for the duty of care as to both sides is set forth in Article 4A and its limitation of liability. *See* *Ma*, 597 F.3d at 89–90 (interpreting Article 4A to displace common law claims, such as negligence, where Article 4A has already specified the relevant duties and "protect[ions] against the type of underlying injury or misconduct alleged in a claim"); *Donmar Enters., Inc. v. S. Nat'l Bank of N.C.*, 64 F.3d 944, 949–50 (4th Cir.1995) (holding that negligence claims are in conflict with, and therefore displaced by, Article 4A); *cf.* *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 161 (1st Cir.2011) (where Maine law is clear that certain damages on given facts are not available regardless of theory pled, Maine law will not under new cause of action allow such damages). So we affirm the dismissal of the negligence claims.

> FN16. This case is not like *Regions Bank* in the sense that there a beneficiary bank accepted funds it knew or had reason to know were fraudulently obtained, and the court held other state law remedies for fraud were not inconsistent with Article 4A. As the court said:
>
> > Interpreting Article 4A in a manner that would allow a beneficiary bank to accept funds when it knows or should know that they were fraudulently obtained, would allow banks to use Article 4A as a shield for fraudulent activity. It could hardly have been the intent of the drafters to enable a party to succeed in engaging in fraudulent activity, so long as it complied with the provisions of Article 4A.
>
> *Regions Bank v. Provident Bank, Inc.*, 345 F.3d 1267, 1276 (11th Cir.2003).

IV.

We reverse the district court's grant of summary judgment in favor of the bank, and affirm the district court's denial of Patco's motion for summary judgment. We remand for further proceedings in accordance with this opinion. On remand the parties may wish to consider whether it would be wiser to invest their resources in resolving this matter by agreement.

No fees are awarded; each side shall bear its own costs.

C.A.1 (Me.),2012.
Patco Const. Co., Inc. v. People's United Bank
684 F.3d 197

END OF DOCUMENT