community BANKER

January/February, 2014

Welcome to the January/ February issue of the COMMUNITY BANKERS' ADVISOR.

The ADVISOR is prepared by attorneys at Olson & Burns P.C. to provide information pertaining to legal developments affecting the field of banking. In order to accomplish this objective, we welcome any comments our readers have regarding the content and format of this publication. Please address your comments to:

Community Bankers' Advisor
c/o Olson & Burns P.C.
P.O. Box 1180
Minot, ND 58702-1180

olsonpc@minotlaw.com

Also, visit our web site at:
www.minotlaw.com

The attorneys at Olson & Burns represent a wide range of clients in the financial and commercial areas. Our attorneys represent more than 30 banks throughout North Dakota.

YOU ARE ASKING. . .

Q: We have a deposit account with an authorized signer - it's not a joint account - and the account has an overdraft. Can the authorized signer be held liable for overdrafts? As far as we can tell, the signer hasn't been acting outside the scope of her authority or done anything illegal.

A: If you do not have an account agreement in which the authorized signer agreed to be liable for overdrafts (and authorized signers typically do not agree to that), the authorized signer *isn't generally liable* if he or she was acting within the scope of his or her authority from the owner of the account. The authorized signer is ordinarily protected from liability in such cases. In other words, you can't set off the authorized signer's savings account or anything like that.

Q: Is there any legal reason to require an individual natural person to use his or her personal name on a sole proprietorship account instead of the business name? For example, is it ok to use "Teddy Bear Daycare" rather than "Debbie Smith, D/B/A Teddy Bear Daycare"? We understand the name mismatch issue with the IRS and the SSN, but this will not be an interest bearing account.

A: One reason is that the FDIC requires that account records reflect the actual and true ownership of accounts. Another reason we can think of off the top of our heads is the need to be able to determine true account ownership if ever the bank is served with legal process such as a garnishment, a tax levy, a writ of execution, a subpoena, or whatever.

Q: We no longer know everyone who enters our bank. We don't want to be jerks, but we are considering posting signs on the door requesting that customers remove caps, hats, hoods and sunglasses before entering the bank. Do we have a right to do this?

O&B ATTORNEYS

OLSON & BURNS P.C.
17 FIRST AVENUE S.E. • P.O. BOX 1180 • MINOT, NORTH DAKOTA 58702-1180
TELEPHONE (701) 839-1740 • FACSIMILE (701) 838-5315 • E-MAIL: olsonpc@minotlaw.com

A: You have the right to do this. Bank robbers rely on these items to conceal their identity. By requiring headgear and sunglasses to be removed, bank surveillance cameras are much more effective. The sign can simply state something like

> For the safety of all customers and bank employees, please remove all caps, hats, hoods, and sunglasses before entering the bank. Thank you.

Some customers will ask questions, but once they are made aware of the reason, they should understand. The bank should also recognize that some customers might have good reason for not complying, such as someone wearing sunglasses due to cataracts or other eye problems or wearing a hat to hide hair loss from chemotherapy. If customers forget to take off caps or sunglasses when they come in, the bank can decide whether it wants to ask customers to comply. Most robbers wear caps or hoods and sunglasses and just quietly hand the teller a note demanding money. They don't want to draw attention to themselves, and maybe the sign alone will deter a would-be bank robber. Perhaps he'll realize that he'll draw attention to himself if he's the only one in the bank with his hood up and sunglasses on. ■

CASES BANKS SHOULD BE AWARE OF (File Under "Something Else to Worry About")

Employee Sexual Harassment by Customer

The EEOC sued, and recently settled with, a Virginia healthcare group that it claimed violated federal law by subjecting a female employee to a sexually hostile work environment. According to the EEOC's lawsuit, Karen Ross, who worked as a receptionist at the facility, was subjected to sexual harassment by a male patient from April to December 2009, and again from June to September 2010. The suit alleges that the harassment included unwelcome sexual comments, such as the patient inviting Ross to "run away with" him, telling Ross that he was "visualizing [her] naked," and suggesting that Ross have sex with him. The suit further alleges that the comments were made both in person, when the patient visited the facility where Ross worked, and by telephone when the patient called in to the facility. The EEOC said that Ross complained to her supervisor about the patient's sexual harassment, but the supervisor did nothing to stop the abusive conduct. Sexual harassment is a form of sex discrimination that violates Title VII of the Civil Rights Act of 1964. "Once an employer is put on notice that any of its employees are being subjected to sexual harassment, it must take prompt corrective action to stop it," said an EEOC lawyer. "This is true regardless of whether the harasser is a co-worker, her supervisor or a third party. The EEOC is committed to using all available means, including litigation, to combat sexual harassment in the workplace."

To settle the charges that it violated Title VII, the healthcare group agreed to pay Ross $30,000 and provide her with a letter of reference. In addition, the company promised to refrain from future discrimination or retaliation in violation of Title VII. For a three-year period, it will report to the EEOC at six-month intervals about any complaints made to the company regarding sexual harassment, with an explanation of the action taken in response. A revised sexual harassment policy – including a statement that sexual harassment of employees by customers and third parties is prohibited under company policy and federal law – also must be distributed to current employees and future employees, as well as posted in the workplace, as part of the settlement. *Additionally*, the company is also required to provide annual training to all employees, including an explanation of Title VII and the rights of employees to be free from third-party sexual harassment.

Why are we telling you this? Because federal law says that harassment in the workplace can be committed not just by supervisors and coworkers, but by third parties such as customers, patients, clients, delivery people, or repair workers. If it crops up in your bank, even if the perpetrator is your longtime best customer, put a stop to it. EEOC v. Southwest Virginia Community Health System, Inc., Consent Decree, (C.C.D.W.Vir., Roanoke Div.) (No. 7:12cv424) (Oct. 25, 2013).

ACH Fraud

In what has been called a "landmark" decision, the 1st Circuit Court of Appeals held in Patco Construction Company, Inc. v. People's United Bank that Ocean Bank may be required to reimburse its customer, Patco Construction Co., after $588,851.26 had been taken from its bank account via unauthorized transfers. This opinion reversed the decision of the lower court that had granted summary judgment in the bank's favor.

Over seven days in May 2009, Ocean Bank, a Maine community bank, authorized six apparently fraudulent withdrawals using Automated Clearing House, totaling $588,851.26, from Patco's account after the perpetrators correctly supplied Patco's customized answers to security questions. Patco claimed that the fraudulent transfers were caused by the Zeus malware, which can capture authentication credentials enabling criminals to initiate

their own transfers. In its decision, the appeals court pointed to a mistake in that Ocean Bank decided to initiate "challenge questions" for any transactions for its customers valued at more than $1. Challenge questions are often used in authentication systems and require a user to enter additional information aside from a login or password, such as the name of the first street a person lived on or the model of his first car. Because the answers to the challenge questions were displayed every time Patco made a transfer, this "increased the risk that such answers would be compromised by keyloggers or other malware that would capture that information for unauthorized uses," according to the ruling.

The court also found that Ocean Bank was not monitoring its transactions for fraud nor notifying customers before a suspicious transaction was allowed to proceed, both capabilities that it had with its security system. The bad guys made the withdrawals through the Bank's eBanking platform using the login credentials, including the correct password and answers to security questions, of a Patco employee. Patco mainly used the Bank's eBanking service to meet its weekly payroll, initiating transactions on generally the same day each week, from the same computer and IP address, and in similar amounts. The fraudulent transactions were not typical in that they were initiated on consecutive days, from different computers and a different IP address, in amounts much greater than Patco's usual transactions, and involved payees to whom Patco had never before sent funds to from this account. The Bank's eBanking security system, provided by Jack Henry & Associates and known as "NetTeller", flagged each of these transactions as unusually "high-risk", but the Bank failed to manually monitor the system's fraud detection reports. The bank's security system did not notify its commercial customers of this information and allowed the payments to go through. Patco discovered the fraudulent transfers six days after the first transaction when the Bank notified it that one of the payments had been automatically returned because the payee's account number was invalid. Ocean Bank was able to block or recover $243,406.83, leaving a loss to Patco of $345,444.43.

Patco sued, claiming, among other things, that the Bank should bear the loss of the unrecovered funds, among other reasons, because the Bank's eBanking security procedures were not commercially reasonable and that Patco had not consented to the procedures. Under Article 4A-201 of the Uniform Commercial Code (enacted in North Dakota as N.D.C.C. § 41-04.1-09), a bank generally bears the risk of loss with respect to an electronic payment order that is not authorized by its commercial customer. However, a bank may *shift* the risk of loss to its customer if the bank accepts the payment order in compliance with commercially reasonable, mutually-agreed-upon security procedures.

Patco argued that the Bank's security procedures were not commercially reasonable, mainly because (i) the Bank required users of its eBanking platform to answer security questions before initiating any transaction of at least $1, which increased the risk that a criminal using "keylogger" software could intercept answers to security questions, and (ii) the Bank failed to implement other available security measures which would have made its security procedures more effective. The lower court rejected these arguments, finding that the security procedures were commercially reasonable notwithstanding the $1 threshold, as they were designed to comply with applicable guidance issued by the Federal Financial Institutions Examination Council (the "FFIEC Guidance") and, though not optimal, were in line with the security features used by other banks with a Jack Henry eBanking security system.

The First Circuit reversed the district court's grant of summary judgment in favor of the Bank on the issue of liability under Article 4A-201, concluding that the Bank's security procedures were not commercially reasonable. The court based its holding on its findings that (i) setting the security question threshold at $1 substantially increased the risk of fraud, particularly for a customer like Patco which made frequent, regular, high-dollar electronic funds transfers, because it provided criminals with more frequent opportunities to capture bank customers' login credentials; (ii) the Bank was on notice of the risks posed by frequent use of challenge questions as a standalone security procedure as early as 2005 but nonetheless failed to implement supplemental security features, even though similarly situated banks had done so; and (iii) the Bank failed to manually monitor the Jack Henry security system's risk scoring reports that indicated that the transactions in question were fraudulent. In the First Circuit's opinion, "These collective failures, taken as a whole, rendered Ocean Bank's security procedures commercially unreasonable."

The appeals court remanded the case to lower court, stating that further hearings will be needed to determine what responsibilities Patco may have had to protect itself during online banking transactions, which doesn't necessarily mean that Patco will be refunded the $345,444.43. The appeals court also advised that, despite its ruling, Patco and Ocean Bank may want to try to settle

the issue out of court.

Things to learn from this case: (1) Both the lower court and the appeals court cited the FFIEC Guidance in their discussion of commercial reasonableness, which suggests the importance of compliance with the FFIEC Guidance. (2) The appeals court made much of Ocean Bank's failure to monitor the risk scoring reports that would have alerted it to the fraud, suggesting that banks that fail to utilize their security systems have a higher risk of being found to have security procedures that are not commercially reasonable. (3) The appeals court appeared to emphasize that *other* community banks were using additional security measures that were fairly easy to implement, indicating that commercial reasonableness is based, in part, on the practices of your peer institutions.

We recommend that banks adopt the most of state of the art technology that their size will allow and should look to similarly-sized banks in North Dakota to examine the type of security measures that they have in place. Also, the FFIEC's 2011 Supplement went into effect in January 2012 and it recommended that banks adapt their security measures to "abnormal" or atypical customer behavior. Whether courts might follow the Patco reasoning or rely on conformance to FFIEC recommendations (and who can predict what will happen), it will be important for banks to implement an individualized security procedure in a way that adapts to changing circumstances. Patco Construction Company, Inc. v. People's United Bank, 684 F3d 197(1st Cir. Me. 2012).

FINAL RULES ON DODD-FRANK REQUIREMENTS FOR HOME OWNERSHIP COUNSELING PUBLISHED BY CFPB

On November 14, the Bureau of Consumer Financial Protection (the "Bureau") published final rules in the *Federal Register* interpreting the homeownership counseling amendments to Regulation Z (Truth in Lending) and Regulation X (Real Estate Settlement Procedures Act). These amendments were designed to implement the requirements of the Dodd-Frank Wall Street Reform and Consumer Protection Act with respect to the Act's requirement that loan applicants receive a list of homeownership counseling organizations.

The final rule provides guidance to lenders in complying with the content requirements of the list of these counseling entities. Previously, the Bureau had specified that lenders may comply with these requirements either by providing information developed and maintained by the Bureau on its website, or by using data made available by the Bureau or by the US Department of Housing and Urban Development for this purpose and by using the data in accordance with instructions provided by these agencies. The requirements for the list of counseling agencies are as follows:

- The list must contain at least 10 HUD-approved counseling agencies.
- The listed agencies must be in the prospective homeowner's location. This requirement is satisfied by providing agencies within the prospective homeowner's zip code.
- The list must contain the name, phone number, street address, city/state/zip, website URL, e-mail address, counseling services provided and languages spoken, for each agency.
- The list must contain the notice set forth in the final rule, informing the borrower of where additional information may be obtained.

Information developed and maintained by the Bureau on its website complies with the above requirements. The final rule is effective January 10, 2014. North Dakota HUD-approved housing counseling agencies may be located at the following website:

http://www.hud.gov/offices/hsg/sfh/hcc/hcs.cfm?webListAction=search&searchstate=ND
