

community BANKER

March/April, 2010

Welcome to the March/April 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: From a regulatory or legal position, what are permissible or acceptable reasons for a customer to request a "stop payment" on a check? We have input stop payments for some pretty flimsy reasons.

A: N.D.C.C. § 41-04-34 (U.C.C. § 4-403) sets out the rules for a stop payment request. The short answer to your question is that the statute does not define any "acceptable" or "permissible" reasons to issue a stop payment order. All it says is that the customer has the right to stop the payment of the check -- it does not give the bank the duty or the authority to decide whether or not the reason is a good one. As long as the customer makes the request in a timely manner, and in the manner described in the deposit contract with the customer, the bank is obligated to act on the customer's order. As a matter of fact, this section is entitled "The Customer's Right to Stop Payment." You may ask the reason for stopping payment just for your records, but even if you think it's a dumb reason (or even if they refuse to give you a reason) you are still obligated to act on the customer's request. In the long run, it is your bank, however, and you always have the right to close an account if you think a customer is managing his account in a dishonest or unsatisfactory manner. (Or so your account agreement should provide.)



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

Q: Four months after a stop payment order was out of the system, we paid a check that had previously had a stop payment order on it. The check was returned for "Payment Stopped in March, 2009." What is the bank's liability here, if any?

A: Under N.D.C.C. § 41-04-34(2), a written stop payment is valid for only six months. The stop payment lapses after that time. The relevant section provides as follows:

2. A stop order is effective for six months after the time it is received, but it lapses after fourteen calendar days if the original order was oral and was not confirmed in writing within that period. A stop order may be renewed for additional six-month periods by a writing given to the bank within a period during which the stop order is effective.

As you can see from the underlined language, if the customer wants to continue the stop payment after six months, he or she can renew the stop payment order for an additional six-month period. (Review the language on your stop payment form and see if it is clear about this.) Assuming that your stop payment forms were clear that they were effective for six months, if you paid a check after the first order expired you have no liability under the language of the statute.

In the old days, this six-month time period was sensible because a check that was more than six months old was "stale dated" and not properly payable anyway. Now, banks may pay what would have been "stale dated" checks if they so choose (but it must be done in good faith). N.D.C.C. § 41-04-35 (U.C.C. § 4-404) provides that

A bank is under no obligation to a customer having a checking account to pay a check, other than a certified check, which is presented more than six months after its date, but it may charge its customer's

account for a payment made thereafter in good faith.

Consider the circumstances when you are presented a check older than six months. If you know that the check was obtained via fraud, sale of damaged goods, etc., the customer may claim your payment of the check was not made "in good faith."

Q: We had a customer come in to cash a check but the written word amount of the check was written in Bosnian. Nobody at our branch reads or speaks Bosnian at all, let alone well enough to know if it was written to correspond to the numerical amount. We requested that the customer bring the check back with the written amount in English. Our question is, will a check be returned if it is in another language?

A: That is a good question, one that we do not know the answer to. We think that it is unlikely that a check would be returned solely because it is not written in English. Despite the fact that the amount in words controls when there's a discrepancy between that amount and the amount in numerals, we understand that most automated check processing is based on the amount in numerals. We suspect that the amount written in words is rarely examined by a drawee bank. Having said all that, however, if your bank is being asked to cash a check, your bank gets to set the rules on how it reviews that particular check and whether it will accept a check when the amount might be in question. Your inability to tell if the numerals and the written numbers correspond seem to be as good a reason as any to refuse to cash the check.

Q: We want to hand out to customers a little "tips" sheet on what to do if victimized by identity theft or credit fraud. What are the basics, easily understood?

A: If you believe that you are a victim of identity theft or credit fraud, it is recommended that you take the following steps:

* Contact any one of the three major credit bureaus (Equifax, TransUnion, Experian) and request that a fraud alert be placed on your credit

file. Once the credit bureau is notified, they will notify the other bureaus.

- * Notify the credit card issuer of the stolen card (if applicable).
- * Notify the bank of the stolen checks or check card (if applicable).
- * File a police report.
- * Contact the Social Security Administration if someone is using your Social Security number.
- * Contact the Federal Trade Commission (FTC) hotline 800-438-4338 and file a complaint. The FTC does not resolve individual consumer problems itself, but your complaint may lead to law enforcement action. It also has an ID Theft Affidavit that you can download from their Web site: www.ftc.com.
- * Check your credit report for any accounts that you do not recognize. Check this periodically since some accounts are not reflected immediately.

VIOLATION OF BANK POLICY -- NOW WHAT?

You have your compliance-required security program in place, but are you keeping in mind that internal investigations are a vital part of a security program? It's a serious matter when an employee is alleged to be violating bank policy. What are commonly called 'insider threats' can cause more damage than thieves from the outside, and, they are far more common. These threats come in many different forms, including but not limited to:

- * Accounting fraud
- * Outright theft of physical assets
- * Unauthorized access in order to manipulate data or to sell it
- * Threats, sexual harassment or other inappropriate forms of behavior

Internal investigations aim to uncover the truth

about alleged misconduct within the bank, but it must do so without compromising the relationship with innocent employees or unnecessarily damaging anyone's reputation. That calls for good planning, consistent execution, analytical skill, sensitivity, and a solid grasp of the legalities involved.

Generally, the investigation will, depending on the threat, encompass collection and examination of written or recorded evidence, interviews with suspects and witnesses, and computer and network forensics. It may also require consultation with managers, human resources and legal personnel, and maybe law enforcement. The people involved and the course of action should be **only those necessary** to handle the particular case. In other words, don't involve staff or outsiders that are not necessary to your investigation. This discussion does not address the regulatory aspect of employee misconduct, but is from a practical legal perspective.

(1) **Have clear policies.** Your policy should set the appropriate personnel and procedures for internal investigations at your bank. A clearly-written policy will help you achieve a successful and correct outcome, avoid common blunders, ensure that proper documentation is kept, and, it is hoped, keep you out of a lawsuit.

(2) **Document your work.** This includes documenting your compliance with your own policies. In the event that the subject of the investigation files a lawsuit against you, you will need to show the judge that you behaved responsibly, correctly, and legally throughout whole procedure.

(3) **Put it in writing.** Give your suspect what we call, for lack of a better term, a "confirmatory memo." Usually, a verbal complaint or accusation is made, but following up with a carefully-thought-out confirmatory memo to the accused clarifies what it is that you believe the suspect did.

(4) **Handle witness intimidation.** We aren't talking about the Mafia here, but some employee/witnesses might feel intimidated by the suspect just because he or she is in the building. Watch that the accused (or management) does not badger or try to influence witnesses in an attempt to affect the outcome of the

investigation. Keep the investigation confidential (the suspect doesn't need to know who you are talking to), and consider removing your suspect from the bank through a paid suspension.

(5) **Create an interview team** and split the duties. In a team interview, one person may ask questions while the other simply takes notes and records observations without commenting. Prepare opening and closing remarks and a set of questions, and ask necessary followup questions. Keep your question sheets and any notes or recordings of the interviews themselves. Be sure to tell the employee that the meeting is being recorded for *everyone's* protection. Internal investigations often involve interviews with employees who are not suspects. You may want to let that employee know that he is not a suspect, which may cause him to give more candid answers.

(6) **Set a time frame for the investigation.** Quick and appropriate action can help head off future legal challenges and also minimize negative impact on morale.

(7) **Gather evidence relevant to the infraction**, including personnel files, telephone records, expense account records, computerized personnel information, appointment calendars, time cards, building entrance/exit records, computer disks and hard drive, e-mail records and voice mail records.

(8) **Investigative techniques** that have a high legal risk should *first* be discussed with legal counsel and should require high-level approval include internal audits, fingerprinting, handwriting analysis, surveillance, lie detector tests, searches of private property, and electronic monitoring. If it comes to this, it really sounds like law enforcement should be involved.

There are other considerations specific to your bank, your policy, and the alleged violation -- think about them. Finally, again, keep the investigation confidential and don't involve anyone who doesn't need to be involved.

DISCLAIMER

COMMUNITY BANKERS' ADVISOR is designed to share ideas and developments related to the field of banking. It is not intended as legal advice and nothing in the COMMUNITY BANKERS' ADVISOR should be relied upon as legal advice in any particular matter. If legal advice or other expert assistance is needed, the services of competent, professional counsel should be sought.