PROPOSED AMENDMENTS RELATING TO PAYMENTS ISSUES

CONTENTS

SECTION 3-105. 2
SECTION 3-309. 2
SECTION 3-604. 4
SECTION 4–209 5
SECTION 4–406. 6
SECTION 4A-103. 12
SECTION 4A-104. 13
SECTION 4A-201. 18
SECTION 4A-202. 19
SECTION 4A-203. 21
SECTION 4A-206. 28
SECTION 4A-207. 30
SECTION 4A-208. 33

SECTION 3-105. ISSUE OF INSTRUMENT.

(a) "Issue" means the first delivery or electronic transmission of an instrument by the maker or drawer, whether to a holder or nonholder, for the purpose of giving rights on the instrument to any person.

(b) An unissued instrument, or an unissued incomplete instrument that is completed, is binding on the maker or drawer, but nonissuance is a defense. An instrument that is conditionally issued or is issued for a special purpose is binding on the maker or drawer, but failure of the condition or special purpose to be fulfilled is a defense.

(c) "Issuer" applies to issued and unissued instruments and means a maker or drawer of an instrument.

Official Comment

1. Under former Section 3–102(1)(a) "issue" was defined as the first delivery to a "holder or a remitter" but the term "remitter" was neither defined nor otherwise used. In revised Article 3, Section 3–105(a) defines "issue" more broadly to include the first delivery to anyone by the drawer or maker for the purpose of giving rights to anyone on the instrument. "Delivery" with respect to instruments is defined in ~~Section 1–201(14)~~ Section 1-201(b)(15) as meaning "voluntary transfer of possession."

Subsection (a) permits an instrument to be issued by an electronic transmission, rather than by delivery. Thus, for example, a drawer might write and sign a check, take a photograph of the check, and send the photograph to the drawee for processing electronically, and destroy the original check. Such a check is "issued" and hence can be enforced pursuant to this Article.

2. Subsection (b) continues the rule that nonissuance, conditional issuance or issuance for a special purpose is a defense of the maker or drawer of an instrument. Thus, the defense can be asserted against a person other than a holder in due course. The same rule applies to nonissuance of an incomplete instrument later completed.

3. Subsection (c) defines "issuer" to include the signer of an unissued instrument for convenience of reference in the statute.

SECTION 3-309. ENFORCEMENT OF LOST, DESTROYED, OR STOLEN INSTRUMENT.

(a) A person not in possession of an instrument is entitled to enforce the instrument if:

(1) the person seeking to enforce the instrument:

(A) was entitled to enforce the instrument when loss of possession occurred; or

(B) has directly or indirectly acquired ownership of the instrument from a person who was entitled to enforce the instrument when loss of possession occurred;

(2) the loss of possession was not the result of a transfer by the person or a lawful seizure; and

(3) the person cannot reasonably obtain possession of the instrument because the instrument was destroyed, its whereabouts cannot be determined, or it is in the wrongful possession of an unknown person or a person that cannot be found or is not amenable to service of process.

(b) A person seeking enforcement of an instrument under subsection (a) must prove the terms of the instrument and the person's right to enforce the instrument. If that proof is made, Section 3-308 applies to the case as if the person seeking enforcement had produced the instrument. The court may not enter judgment in favor of the person seeking enforcement unless it finds that the person required to pay the instrument is adequately protected against loss that might occur by reason of a claim by another person to enforce the instrument. Adequate protection may be provided by any reasonable means.

Official Comment

1. Section 3–309 is a modification of former Section 3–804. The rights stated are those of "a person entitled to enforce the instrument" at the time of loss rather than those of an "owner" as in former Section 3–804. Under subsection (b), judgment to enforce the instrument cannot be given unless the court finds that the defendant will be adequately protected against a claim to the instrument by a holder that may appear at some later time. The court is given discretion in determining how adequate protection is to be assured. Former Section 3–804 allowed the court to "require security indemnifying the defendant against loss." Under Section 3–309 adequate protection is a flexible concept. For example, there is substantial risk that a holder in due course may make a demand for payment if the instrument was payable to bearer when it was lost or stolen. On the other hand if the instrument was payable to the person who lost the instrument and that person did not indorse the instrument, no other person could be a holder of the instrument. In some cases there is risk of loss only if there is doubt about whether the facts alleged by the person who lost the instrument are true. Thus, the type of adequate protection that is reasonable in the circumstances may depend on the degree of certainty about the facts in the case.

2. Subsection (a) is intended to reject the result in Dennis Joslin Co. v. Robinson Broadcasting Corp., 977 F. Supp. 491 (D.D.C. 1997). A transferee of a lost instrument need prove only that its transferor was entitled to enforce, not that the transferee was in possession at

the time the instrument was lost. The protections of subsection (a) should also be available when instruments are lost during transit, because whatever the precise status of ownership at the point of loss, either the sender or the receiver ordinarily would have been entitled to enforce the instrument during the course of transit. The amendments to subsection (a) are not intended to alter in any way the rules that apply to the preservation of checks in connection with truncation or any other expedited method of check collection or processing.

3. A security interest may attach to the right of a person not in possession of an instrument to enforce the instrument. Although the secured party may not be the owner of the instrument, the secured party may nevertheless be entitled to exercise its debtor's right to enforce the instrument by resorting to its collection rights under the circumstances described in Section 9-607. This section does not address whether the person required to pay the instrument owes any duty to a secured party that is not itself the owner of the instrument.

4. The destruction of a check in connection with a truncation process in which information is extracted from the check and then transmitted for payment does not, by itself, prevent application of this section. *See* Section 3-604 comment 1.

Example: The payee of a check creates an image of the check, destroys the check, and transmits the image for payment. Due to an error in transmission, the depositary bank never receives the transmission. If the payee can prove the terms of the check and otherwise satisfy the requirements of this section, the payee may enforce the check. The result would be different if there were no error in the transmission and the payor discharged its obligation on the check.

SECTION 3-604. DISCHARGE BY CANCELLATION OR RENUNCIATION.

(a) A person entitled to enforce an instrument, with or without consideration, may discharge the obligation of a party to pay the instrument (i) by an intentional voluntary act, such as surrender of the instrument to the party, destruction, mutilation, or cancellation of the instrument, cancellation or striking out of the party's signature, or the addition of words to the instrument indicating discharge, or (ii) by agreeing not to sue or otherwise renouncing rights against the party by a signed record.

(b) Cancellation or striking out of an indorsement pursuant to subsection (a) does not affect the status and rights of a party derived from the indorsement.

(c) In this section, "signed," with respect to a record that is not a writing, includes the attachment to or logical association with the record of an electronic symbol, sound, or process with the present intent to adopt or accept the record.

Official Comment

Section 3–604 replaces former Section 3–605.

1. The destruction of a check in connection with a truncation process in which information is extracted from the check and then transmitted for payment is not within the scope of this section and does not by itself discharge the obligation of a party to pay the instrument.

SECTION 4–209. ENCODING AND RETENTION WARRANTIES.

(a) A person who encodes information on or with respect to an item after issue warrants to any subsequent collecting bank and to the payor bank or other payor that the information is correctly encoded. If the customer of a depositary bank encodes, that bank also makes the warranty.

(b) A person who undertakes to retain an item pursuant to or in connection with an agreement for electronic presentment warrants:

(1) to any subsequent collecting bank and to the payor bank or other payor that retention and presentment of the item comply with the agreement; and

(2) to the depositary bank, payor bank, and the drawer that the retained item will not also be presented for payment.

If a customer of a depositary bank undertakes to retain an item, that bank also makes ~~this~~ the warranty under paragraph (1).

(c) A person to whom warranties are made under this section and who took the item in good faith may recover from the warrantor as damages for breach of warranty an amount equal to the loss suffered as a result of the breach, plus expenses and loss of interest incurred as a result of the breach.

Official Comment

1. Encoding and retention warranties are included in Article 4 because they are unique to the bank collection process. These warranties are breached only by the person doing the encoding or retaining the item and not by subsequent banks handling the item. Encoding and check retention may be done by customers who are payees of a large volume of checks; hence, this section imposes warranties on customers as well as banks. If a customer encodes or retains, the depositary bank is also liable for any breach of this warranty.

2. A misencoding of the amount on the MICR line is not an alteration under Section 3–407(a) which defines alteration as changing the contract of the parties. If a drawer wrote a check for $2,500 and the depositary bank encoded $25,000 on the MICR line, the payor bank could debit the drawer's account for only $2,500. This subsection would allow the payor bank to hold the depositary bank liable for the amount paid out over $2,500 without first pursuing the person who received payment. Intervening collecting banks would not be liable to the payor bank for the depositary bank's error. If a drawer wrote a check for $25,000 and the depositary bank encoded $2,500, the payor bank becomes liable for the full amount of the check. The payor bank's rights against the depositary bank depend on whether the payor bank has suffered a loss. Since the payor bank can debit the drawer's account for $25,000, the payor bank has a loss only to the extent that the drawer's account is less than the full amount of the check. There is no requirement that the payor bank pursue collection against the drawer beyond the amount in the drawer's account as a condition to the payor bank's action against the depositary bank for breach of warranty. See Georgia Railroad Bank & Trust Co. v. First National Bank & Trust, 229 S.E.2d 482 (Ga.App.1976), aff'd, 235 S.E.2d 1 (Ga.1977), and First National Bank of Boston v. Fidelity Bank, National Association, 724 F.Supp. 1168 (E.D.Pa.1989).

3. A person retaining items under an electronic presentment agreement (Section 4–110) warrants that it has complied with the terms of the agreement regarding its possession of the item and its sending a proper presentment notice. If the keeper is a customer, its depositary bank also makes this warranty.

4. Although a drawee would not normally be a party to an electronic presentment agreement, and thus would not retain an item "pursuant to" such an agreement, a drawee might retain an item "in connection with" such an agreement entered into by the depositary bank. Such a drawee makes the warranties provided for in subsection (b).

Reporter's Note

Section 4-110(c) provides that if presentment is made by presentment notice – that is, if presentment is made electronically – a reference in Article 4 to "item" or "check" means the presentment notice unless the context otherwise indicates. The Drafting Committee should consider whether the proposed amendment to subsection (b), and specifically its reference to "the retained item," is sufficiently clear of a situation in which "context that otherwise requires."

SECTION 4–406. CUSTOMER'S DUTY TO DISCOVER AND REPORT UNAUTHORIZED SIGNATURE OR ALTERATION.

(a) A bank that sends or makes available to a customer a statement of account showing payment of items for the account shall either return or make available to the customer the items paid or provide information in the statement of account sufficient to allow the customer

reasonably to identify the items paid. The statement of account provides sufficient information if the item is described by item number, payee, amount, date of the item, and date of payment.

(b) If the items are not returned to the customer, the person retaining the items shall either retain the items or, if the items are destroyed, maintain the capacity to furnish legible copies of the items until the expiration of seven years after receipt of the items. A customer may request an item from the bank that paid the item, and that bank must provide in a reasonable time either the item or, if the item has been destroyed or is not otherwise obtainable, a legible copy of the item.

(c) If a bank sends or makes available a statement of account or items pursuant to subsection (a), the customer must exercise reasonable promptness in examining the statement or the items to determine whether any payment was not authorized because of an alteration of an item or because a purported signature by or on behalf of the customer was not authorized. If, based on the statement or items provided, the customer should reasonably have discovered the unauthorized payment, the customer must promptly notify the bank of the relevant facts.

(d) If the bank proves that the customer failed, with respect to an item, to comply with the duties imposed on the customer by subsection (c), the customer is precluded from asserting against the bank:

(1) the customer's unauthorized signature or any alteration on the item, if the bank also proves that it suffered a loss by reason of the failure; and

(2) the customer's unauthorized signature or alteration by the same wrongdoer on any other item paid in good faith by the bank if the payment was made before the bank received notice from the customer of the unauthorized signature or alteration and after the customer had been afforded a reasonable period of time, not exceeding 30 days, in which to examine the item or statement of account and notify the bank.

(e) If subsection (d) applies and the customer proves that the bank failed to exercise ordinary care in paying the item and that the failure substantially contributed to loss, the loss is allocated between the customer precluded and the bank asserting the preclusion according to the extent to which the failure of the customer to comply with subsection (c) and the failure of the bank to exercise ordinary care contributed to the loss. If the customer proves that the bank did not pay the item in good faith, the preclusion under subsection (d) does not apply.

(f) Without regard to care or lack of care of either the customer or the bank, a customer who does not within one year after the statement or items are made available to the customer (subsection (a)) discover and report the customer's unauthorized signature on or any alteration on the item is precluded from asserting against the bank the unauthorized signature or alteration. If there is a preclusion under this subsection, the payor bank may not recover for breach of warranty under Section 4–208 with respect to the unauthorized signature or alteration to which the preclusion applies.

Official Comment

1. Under subsection (a), if a bank that has paid a check or other item for the account of a customer makes available to the customer a statement of account showing payment of the item, the bank must either return the item to the customer or provide a description of the item sufficient to allow the customer to identify it. Under subsection (c), the customer has a duty to exercise reasonable promptness in examining the statement or the returned item to discover any unauthorized signature of the customer or any alteration and to promptly notify the bank if the customer should reasonably have discovered the unauthorized signature or alteration.

The duty stated in subsection (c) becomes operative only if the "bank sends or makes available a statement of account or items pursuant to subsection (a)." A bank is not under a duty to send a statement of account or the paid items to the customer; but, if it does not do so, the customer does not have any duties under subsection (c). A bank that permits a customer to access the customer's account online and to view there the activity associated with the account does not thereby make available a "statement of account." A "statement of account" is a periodic record, not a continuous record, of the debits and credits to an account.

Under subsection (a), a statement of account must provide information "sufficient to allow the customer reasonably to identify the items paid." If the bank supplies its customer with an image of the paid item, it complies with this standard. But a safe harbor rule is provided. The bank complies with the standard of providing "sufficient information" if "the item is described by item number, amount, and date of payment." This means that the customer's duties under subsection (c) are triggered if the bank sends a statement of account complying with the safe harbor rule without returning the paid items. A bank does not have to return the paid items unless it has agreed with the customer to do so. Whether there is such an agreement depends upon the particular circumstances. See Section 1–201(3). If the bank elects to provide the minimum information that is "sufficient" under subsection (a) and, as a consequence, the customer could not "reasonably have discovered the unauthorized payment," there is no preclusion under subsection (d). If the customer made a record of the issued checks on the check stub or carbonized copies furnished by the bank in the checkbook, the customer should usually be able to verify the paid items shown on the statement of account and discover any unauthorized or altered checks. But there could be exceptional circumstances. For example, if a check is altered by changing the name of the payee, the customer could not normally detect the fraud unless the customer is given the paid check or the statement of account discloses the name of the

payee of the altered check. If the customer could not "reasonably have discovered the unauthorized payment" under subsection (c) there would not be a preclusion under subsection (d).

The safe harbor provided by subsection (a) serves to permit a bank, based on the state of existing technology, to trigger the customer's duties under subsection (c) by providing a "statement of account showing payment of items" without having to return the paid items, in any case in which the bank has not agreed with the customer to return the paid items. The safe harbor does not, however, preclude a customer under subsection (d) from asserting its unauthorized signature or an alteration against a bank in those circumstances in which under subsection (c) the customer should not "reasonably have discovered the unauthorized payment." Whether the customer has failed to comply with its duties under subsection (c) is determined on a case-by-case basis.

~~The provision in subsection (a) that a statement of account contains "sufficient information if the item is described by item number, amount, and date of payment" is based upon the existing state of technology. This information was chosen because it can be obtained by the bank's computer from the check's MICR line without examination of the items involved. The other two items of information that the customer would normally want to know -- the name of the payee and the date of the item -- cannot currently be obtained from the MICR line. The safe harbor rule is important in determining the feasibility of payor or collecting bank check retention plans. A customer who keeps a record of checks written, e.g., on the check stubs or carbonized copies of the checks supplied by the bank in the checkbook, will usually have sufficient information to identify the items on the basis of item number, amount, and date of payment. But customers who do not utilize these record-keeping methods may not. The policy decision is that accommodating customers who do not keep adequate records is not as desirable as accommodating customers who keep more careful records. This policy results in less cost to the check collection system and thus to all customers of the system. It is expected that technological advances such as image processing may make it possible for banks to give customers more information in the future in a manner that is fully compatible with automation or truncation systems. At that time the Permanent Editorial Board may wish to make recommendations for an amendment revising the safe harbor requirements in the light of those advances.~~

2. Subsection (d) states the consequences of a failure by the customer to perform its duty under subsection (c) to report an alteration or the customer's unauthorized signature. Subsection (d)(1) applies to the unauthorized payment of the item to which the duty to report under subsection (c) applies. If the bank proves that the customer "should reasonably have discovered the unauthorized payment" (See Comment 1) and did not notify the bank, the customer is precluded from asserting against the bank the alteration or the customer's unauthorized signature if the bank proves that it suffered a loss as a result of the failure of the customer to perform its subsection (c) duty. Subsection (d)(2) applies to cases in which the customer fails to report an unauthorized signature or alteration with respect to an item in breach of the subsection (c) duty (See Comment 1) and the bank subsequently pays other items of the customer with respect to which there is an alteration or unauthorized signature of the customer and the same wrongdoer is involved. If the payment of the subsequent items occurred after the customer has had a reasonable time (not exceeding 30 days) to report with respect to the first item and before the

bank received notice of the unauthorized signature or alteration of the first item, the customer is precluded from asserting the alteration or unauthorized signature with respect to the subsequent items.

If the customer is precluded in a single or multiple item unauthorized payment situation under subsection (d), but the customer proves that the bank failed to exercise ordinary care in paying the item or items and that the failure substantially contributed to the loss, subsection (e) provides a comparative negligence test for allocating loss between the customer and the bank. Subsection (e) also states that, if the customer proves that the bank did not pay the item in good faith, the preclusion under subsection (d) does not apply.

Subsection (d)(2) changes former subsection (2)(b) by adopting a 30–day period in place of a 14–day period. Although the 14–day period may have been sufficient when the original version of Article 4 was drafted in the 1950s, given the much greater volume of checks at the time of the revision, a longer period was viewed as more appropriate. The rule of subsection (d)(2) follows pre-Code case law that payment of an additional item or items bearing an unauthorized signature or alteration by the same wrongdoer is a loss suffered by the bank traceable to the customer's failure to exercise reasonable care (See Comment 1) in examining the statement and notifying the bank of objections to it. One of the most serious consequences of failure of the customer to comply with the requirements of subsection (c) is the opportunity presented to the wrongdoer to repeat the misdeeds. Conversely, one of the best ways to keep down losses in this type of situation is for the customer to promptly examine the statement and notify the bank of an unauthorized signature or alteration so that the bank will be alerted to stop paying further items. Hence, the rule of subsection (d)(2) is prescribed, and to avoid dispute a specific time limit, 30 days, is designated for cases to which the subsection applies. These considerations are not present if there are no losses resulting from the payment of additional items. In these circumstances, a reasonable period for the customer to comply with its duties under subsection (c) would depend on the circumstances (Section 1–204(2)) and the subsection (d)(2) time limit should not be imported by analogy into subsection (c).

3. Subsection (b) applies if the items are not returned to the customer. Check retention plans may include a simple payor bank check retention plan or the kind of check retention plan that would be authorized by a truncation agreement in which a collecting bank or the payee may retain the items. Even after agreeing to a check retention plan, a customer may need to see one or more checks for litigation or other purposes. The customer's request for the check may always be made to the payor bank. Under subsection (b) retaining banks may destroy items but must maintain the capacity to furnish legible copies for seven years. A legible copy may include an image of an item. This Act does not define the length of the reasonable period of time for a bank to provide the check or copy of the check. What is reasonable depends on the capacity of the bank and the needs of the customer. This Act does not specify sanctions for failure to retain or furnish the items or legible copies; this is left to other laws regulating banks. See Comment 3 to Section 4–101. Moreover, this Act does not regulate fees that banks charge their customers for furnishing items or copies or other services covered by the Act, but under principles of law such as unconscionability or good faith and fair dealing, courts have reviewed fees and the bank's exercise of a discretion to set fees. Perdue v. Crocker National Bank, 38 Cal.3d 913 (1985) (unconscionability); Best v. United Bank of Oregon, 739 P.2d 554, 562–566 (1987)

(good faith and fair dealing). In addition, Section 1–203 provides that every contract or duty within this Act imposes an obligation of good faith in its performance or enforcement.

4. Subsection (e) replaces former subsection (3) and poses a modified comparative negligence test for determining liability. See the discussion on this point in the Comments to Sections 3–404, 3–405, and 3–406. The term "good faith" is defined in Section 1-201(b)(20) as including "observance of reasonable commercial standards of fair dealing." The connotation of this standard is fairness and not absence of negligence.

The term "ordinary care" used in subsection (e) is defined in Section 3–103(a)(7), made applicable to Article 4 by Section 4–104(c), to provide that sight examination by a payor bank is not required if its procedure is reasonable and is commonly followed by other comparable banks in the area. The case law is divided on this issue. The definition of "ordinary care" in Section 3–103 rejects those authorities that hold, in effect, that failure to use sight examination is negligence as a matter of law. The effect of the definition of "ordinary care" on Section 4–406 is only to provide that in the small percentage of cases in which a customer's failure to examine its statement or returned items has led to loss under subsection (d) a bank should not have to share that loss solely because it has adopted an automated collection or payment procedure in order to deal with the great volume of items at a lower cost to all customers.

5. Several changes are made in former Section 4–406(5). First, former subsection (5) is deleted and its substance is made applicable only to the one-year notice preclusion in former subsection (4) (subsection (f)). Thus if a drawer has not notified the payor bank of an unauthorized check or material alteration within the one-year period, the payor bank may not choose to recredit the drawer's account and pass the loss to the collecting banks on the theory of breach of warranty. Second, the reference in former subsection (4) to unauthorized indorsements is deleted. Section 4–406 imposes no duties on the drawer to look for unauthorized indorsements. Section 4–111 sets out a statute of limitations allowing a customer a three-year period to seek a credit to an account improperly charged by payment of an item bearing an unauthorized indorsement. Third, subsection (c) is added to Section 4–208 to assure that if a depositary bank is sued for breach of a presentment warranty, it can defend by showing that the drawer is precluded by Section 3–406 or Section 4–406(c) and (d). *Revisions approved by the Permanent Editorial Board for the Uniform Commercial Code, March 16, 1991.*

Reporter's Note

The proposed statutory change is offered for discussion purposes only. The proposal essentially takes up the offer previously made in the fifth paragraph of comment 1 to revisit the safe harbor of what constitutes a statement of account as technology changes and makes it easier for banks to provide customers with more information about items paid. It is now customary for banks to provide an image of paid items, and accordingly it seems reasonable to require that the original payee and the date of the item be included in the statement of account.

The proposed amendment to the second paragraph of comment 1 is designed to address how a customer's online access to the customer's account affects the customer's duty to report an unauthorized payment. Specifically, it indicates that providing continuous online access is not sending or making available a statement of account, and thus does not trigger the customer's duty to report. The amendment might not be necessary. That is because the failure to timely

report an unauthorized payment does not necessarily prevent the customer from recovering the amount paid. Instead, the customer is precluded from asserting an unauthorized signature or alteration only if the bank proves that the failure to timely report caused the loss (or another loss due to the same wrongdoer). Given the limited nature of the consequences, the Committee should consider whether it would be appropriate to, in effect, impose on the customer a continuous duty to report unauthorize payments.

If the Committee deems it desirable to specify that the customer's duty to report is not triggered merely by the customer's online access to the customer's account, the Committee might wish to consider whether the approach taken here – an amendment to the comments – is the best approach. For example, the section could be amended state that online access is not a statement of account. However, Section 4-103(a) generally allows the parties to alter the effect of the provisions of Article 4, and thus, unless the Committee were prepared to specify which rules were nonwaivable, *cf.* § 9-602, a bank would by contract be able to require its customer to report unauthorized payments within a short time (*e.g.*, within five days of payment).

SECTION 4A-103. PAYMENT ORDER - DEFINITIONS.

(a) In this Article:

(1) "Payment order" means an instruction of a sender to a receiving bank, transmitted orally, electronically, or in writing, to pay, or to cause another bank to pay, a fixed or determinable amount of money to a beneficiary if:

(i) the instruction does not state a condition to payment to the beneficiary other than time of payment,

(ii) the receiving bank is to be reimbursed by debiting an account of, or otherwise receiving payment from, the sender, and

(iii) the instruction is transmitted by the sender directly to the receiving bank or to an agent, funds-transfer system, or communication system for transmittal to the receiving bank.

(2) "Beneficiary" means the person to be paid by the beneficiary's bank.

(3) "Beneficiary's bank" means the bank identified in a payment order in which an account of the beneficiary is to be credited pursuant to the order or which otherwise is to make payment to the beneficiary if the order does not provide for payment to an account.

(4) "Receiving bank" means the bank to which the sender's instruction is addressed.

(5) "Sender" means the person giving the instruction to the receiving bank.

(b) If an instruction complying with subsection (a)(1) is to make more than one payment to a beneficiary, the instruction is a separate payment order with respect to each payment.

(c) A payment order is issued when it is sent to the receiving bank.

Official Comment

This section is discussed in the Comment following Section 4A-104.

SECTION 4A-104. FUNDS TRANSFER - DEFINITIONS.

In this Article:

(a) "Funds transfer" means the series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order. The term includes any payment order issued by the originator's bank or an intermediary bank intended to carry out the originator's payment order. A funds transfer is completed by acceptance by the beneficiary's bank of a payment order for the benefit of the beneficiary of the originator's payment order.

(b) "Intermediary bank" means a receiving bank other than the originator's bank or the beneficiary's bank.

(c) "Originator" means the sender of the first payment order in a funds transfer.

(d) "Originator's bank" means (i) the receiving bank to which the payment order of the originator is issued if the originator is not a bank, or (ii) the originator if the originator is a bank.

Official Comment

1. Article 4A governs a method of payment in which the person making payment (the "originator") directly transmits an instruction to a bank either to make payment to the person receiving payment (the "beneficiary") or to instruct some other bank to make payment to the beneficiary. The payment from the originator to the beneficiary occurs when the bank that is to pay the beneficiary becomes obligated to pay the beneficiary. There are two basic definitions: "Payment order" stated in Section 4A-103 and "Funds transfer" stated in Section 4A-104. These definitions, other related definitions, and the scope of Article 4A can best be understood in the context of specific fact situations. Consider the following cases:

Case #1. X, which has an account in Bank A, instructs that bank to pay $1,000,000 to Y's account in Bank A. Bank A carries out X's instruction by making a credit of

$1,000,000 to Y's account and notifying Y that the credit is available for immediate withdrawal. The instruction by X to Bank A is a "payment order" which was issued when it was sent to Bank A. Section 4A-103(a)(1) and (c). X is the "sender" of the payment order and Bank A is the "receiving bank." Section 4A-103(a)(5) and (a)(4). Y is the "beneficiary" of the payment order and Bank A is the "beneficiary's bank." Section 4A-103(a)(2) and (a)(3). When Bank A notified Y of receipt of the payment order, Bank A "accepted" the payment order. Section 4A-209(b)(1). When Bank A accepted the order it incurred an obligation to Y to pay the amount of the order. Section 4A-404(a). When Bank A accepted X's order, X incurred an obligation to pay Bank A the amount of the order. Section 4A-402(b). Payment from X to Bank A would normally be made by a debit to X's account in Bank A. Section 4A-403(a)(3). At the time Bank A incurred the obligation to pay Y, payment of $1,000,000 by X to Y was also made. Section 4A-406(a). Bank A paid Y when it gave notice to Y of a withdrawable credit of $1,000,000 to Y's account. Section 4A-405(a). The overall transaction, which comprises the acts of X and Bank A, in which the payment by X to Y is accomplished is referred to as the "funds transfer." Section 4A-104(a). In this case only one payment order was involved in the funds transfer. A one-payment-order funds transfer is usually referred to as a "book transfer" because the payment is accomplished by the receiving bank's debiting the account of the sender and crediting the account of the beneficiary in the same bank. X, in addition to being the sender of the payment order to Bank A, is the "originator" of the funds transfer. Section 4A-104(c). Bank A is the "originator's bank" in the funds transfer as well as the beneficiary's bank. Section 4A-104(d).

Case #2. Assume the same facts as in Case #1 except that X instructs Bank A to pay $1,000,000 to Y's account in Bank B. With respect to this payment order, X is the sender, Y is the beneficiary, and Bank A is the receiving bank. Bank A carries out X's order by instructing Bank B to pay $1,000,000 to Y's account. This instruction is a payment order in which Bank A is the sender, Bank B is the receiving bank, and Y is the beneficiary. When Bank A issued its payment order to Bank B, Bank A "executed" X's order. Section 4A-301(a). In the funds transfer, X is the originator, Bank A is the originator's bank, and Bank B is the beneficiary's bank. When Bank A executed X's order, X incurred an obligation to pay Bank A the amount of the order. Section 4A-402(c). When Bank B accepts the payment order issued to it by Bank A, Bank B incurs an obligation to Y to pay the amount of the order (Section 4A-404 (a)) and Bank A incurs an obligation to pay Bank B. Section 4A-402(b). Acceptance by Bank B also results in payment of $1,000,000 by X to Y. Section 4A-406(a). In this case two payment orders are involved in the funds transfer.

Case #3. Assume the same facts as in Case #2 except that Bank A does not execute X's payment order by issuing a payment order to Bank B. One bank will not normally act to carry out a funds transfer for another bank unless there is a preexisting arrangement between the banks for transmittal of payment orders and settlement of accounts. For example, if Bank B is a foreign bank with which Bank A has no relationship, Bank A can utilize a bank that is a correspondent of both Bank A and Bank B. Assume Bank A issues a payment order to Bank C to pay $1,000,000 to Y's account in Bank B. With respect to this order, Bank A is the sender, Bank C is the receiving bank, and Y is the

beneficiary. Bank C will execute the payment order of Bank A by issuing a payment order to Bank B to pay $1,000,000 to Y's account in Bank B. With respect to Bank C's payment order, Bank C is the sender, Bank B is the receiving bank, and Y is the beneficiary. Payment of $1,000,000 by X to Y occurs when Bank B accepts the payment order issued to it by Bank C. In this case the funds transfer involves three payment orders. In the funds transfer, X is the originator, Bank A is the originator's bank, Bank B is the beneficiary's bank, and Bank C is an "intermediary bank." Section 4A-104 (b). In some cases there may be more than one intermediary bank, and in those cases each intermediary bank is treated like Bank C in Case #3.

As the three cases demonstrate, a payment under Article 4A involves an overall transaction, the funds transfer, in which the originator, X, is making payment to the beneficiary, Y, but the funds transfer may encompass a series of payment orders that are issued in order to effect the payment initiated by the originator's payment order.

In some cases the originator and the beneficiary may be the same person. This will occur, for example, when a corporation orders a bank to transfer funds from an account of the corporation in that bank to another account of the corporation in that bank or in some other bank. In some funds transfers the first bank to issue a payment order is a bank that is executing a payment order of a customer that is not a bank. In this case the customer is the originator. In other cases, the first bank to issue a payment order is not acting for a customer, but is making a payment for its own account. In that event the first bank to issue a payment order is the originator as well as the originator's bank.

2. "Payment order" is defined in Section 4A-103(a)(1) as an instruction to a bank to pay, or to cause another bank to pay, a fixed or determinable amount of money. The bank to which the instruction is addressed is known as the "receiving bank." Section 4A-103(a)(4). "Bank" is defined in Section 4A-105(a)(2). The effect of this definition is to limit Article 4A to payments made through the banking system. A transfer of funds made by an entity outside the banking system is excluded. A transfer of funds through an entity other than a bank is usually a consumer transaction involving relatively small amounts of money and a single contract carried out by transfers of cash or a cash equivalent such as a check. Typically, the transferor delivers cash or a check to the company making the transfer, which agrees to pay a like amount to a person designated by the transferor. Transactions covered by Article 4A typically involve very large amounts of money in which several transactions involving several banks may be necessary to carry out the payment. Payments are normally made by debits or credits to bank accounts. Originators and beneficiaries are almost always business organizations and the transfers are usually made to pay obligations. Moreover, these transactions are frequently done on the basis of very short-term credit granted by the receiving bank to the sender of the payment order. Wholesale wire transfers involve policy questions that are distinct from those involved in consumer-based transactions by nonbanks.

3. Further limitations on the scope of Article 4A are found in the three requirements found in subparagraphs (i), (ii), and (iii) of Section 4A-103(a)(1). Subparagraph (i) states that the instruction to pay is a payment order only if it "does not state a condition to payment to the

beneficiary other than time of payment." An instruction to pay a beneficiary sometimes is subject to a requirement that the beneficiary perform some act such as delivery of documents.

~~For example,~~ **Example:** a New York bank may have issued a letter of credit in favor of X, a California seller of goods to be shipped to the New York bank's customer in New York. The terms of the letter of credit provide for payment to X if documents are presented to prove shipment of the goods. Instead of providing for presentment of the documents to the New York bank, the letter of credit states that they may be presented to a California bank that acts as an agent for payment. The New York bank sends an instruction to the California bank to pay X upon presentation of the required documents. The instruction is not covered by Article 4A because payment to the beneficiary is conditional upon receipt of shipping documents. The function of banks in a funds transfer under Article 4A is comparable to the role of banks in the collection and payment of checks in that it is essentially mechanical in nature. The low price and high speed that characterize funds transfers reflect this fact. Conditions to payment by the California bank other than time of payment impose responsibilities on that bank that go beyond those in Article 4A funds transfers. Although the payment by the New York bank to X under the letter of credit is not covered by Article 4A, if X is paid by the California bank, payment of the obligation of the New York bank to reimburse the California bank could be made by an Article 4A funds transfer. In such a case there is a distinction between the payment by the New York bank to X under the letter of credit and the payment by the New York bank to the California bank. For example, if the New York bank pays its reimbursement obligation to the California bank by a Fedwire naming the California bank as beneficiary (see Comment 1 to Section 4A-107), payment is made to the California bank rather than to X. That payment is governed by Article 4A and it could be made either before or after payment by the California bank to X. The payment by the New York bank to X under the letter of credit is not governed by Article 4A and it occurs when the California bank, as agent of the New York bank, pays X. No payment order was involved in that transaction. In this example, if the New York bank had erroneously sent an instruction to the California bank unconditionally instructing payment to X, the instruction would have been an Article 4A payment order. If the payment order was accepted (Section 4A-209(b)) by the California bank, a payment by the New York bank to X would have resulted (Section 4A-406(a)). But Article 4A would not prevent recovery of funds from X on the basis that X was not entitled to retain the funds under the law of mistake and restitution, letter of credit law or other applicable law.

An instruction to pay might be a component of a so-called "smart contract": a computer program or a transaction protocol intended to execute automatically. The fact that the smart contract itself is subject to a condition does not necessarily mean that an instruction to a payment issued pursuant to that smart contract "state[s] a condition to payment of the beneficiary" within the meaning of Section 4A-102(a)(1)(i). Whether the instruction does state such a condition depends on what the instruction says when it is received by the receiving bank. An instruction that neither grants discretion nor imposes a limitation on payment by the receiving bank does not state a condition to payment. What distinguishes the prior example is that the New York bank's instruction to the California bank did state a condition when the California bank received it.

4. Transfers of funds made through the banking system are commonly referred to as either "credit" transfers or "debit" transfers. In a credit transfer the instruction to pay is given by the person making payment. In a debit transfer the instruction to pay is given by the person receiving payment. The purpose of subparagraph (ii) of subsection (a)(1) of Section 4A-103 is to include credit transfers in Article 4A and to exclude debit transfers. All of the instructions to pay in the three cases described in Comment 1 fall within subparagraph (ii). Take Case #2 as an example. With respect to X's instruction given to Bank A, Bank A will be reimbursed by debiting X's account or otherwise receiving payment from X. With respect to Bank A's instruction to Bank B, Bank B will be reimbursed by receiving payment from Bank A. In a debit transfer, a creditor, pursuant to authority from the debtor, is enabled to draw on the debtor's bank account by issuing an instruction to pay to the debtor's bank. If the debtor's bank pays, it will be reimbursed by the debtor rather than by the person giving the instruction. For example, the holder of an insurance policy may pay premiums by authorizing the insurance company to order the policyholder's bank to pay the insurance company. The order to pay may be in the form of a draft covered by Article 3, or it might be an instruction to pay that is not an instrument under that Article. The bank receives reimbursement by debiting the policyholder's account. Or, a subsidiary corporation may make payments to its parent by authorizing the parent to order the subsidiary's bank to pay the parent from the subsidiary's account. These transactions are not covered by Article 4A because subparagraph (2) is not satisfied. Article 4A is limited to transactions in which the account to be debited by the receiving bank is that of the person in whose name the instruction is given.

If the beneficiary of a funds transfer is the originator of the transfer, the transfer is governed by Article 4A if it is a credit transfer in form. If it is in the form of a debit transfer it is not governed by Article 4A. For example, Corporation has accounts in Bank A and Bank B. Corporation instructs Bank A to pay to Corporation's account in Bank B. The funds transfer is governed by Article 4A. Sometimes, Corporation will authorize Bank B to draw on Corporation's account in Bank A for the purpose of transferring funds into Corporation's account in Bank B. If Corporation also makes an agreement with Bank A under which Bank A is authorized to follow instructions of Bank B, as agent of Corporation, to transfer funds from Customer's account in Bank A, the instruction of Bank B is a payment order of Customer and is governed by Article 4A. This kind of transaction is known in the wire-transfer business as a "drawdown transfer." If Corporation does not make such an agreement with Bank A and Bank B instructs Bank A to make the transfer, the order is in form a debit transfer and is not governed by Article 4A. These debit transfers are normally ACH transactions in which Bank A relies on Bank B's warranties pursuant to ACH rules, including the warranty that the transfer is authorized.

5. The principal effect of subparagraph (iii) of subsection (a) of Section 4A-103 is to exclude from Article 4A payments made by check or credit card. In those cases the instruction of the debtor to the bank on which the check is drawn or to which the credit card slip is to be presented is contained in the check or credit card slip signed by the debtor. The instruction is not transmitted by the debtor directly to the debtor's bank. Rather, the instruction is delivered or otherwise transmitted by the debtor to the creditor who then presents it to the bank either directly or through bank collection channels. These payments are governed by Articles 3 and 4 and federal law. There are, however, limited instances in which the paper on which a check is

printed can be used as the means of transmitting a payment order that is covered by Article 4A. Assume that Originator instructs Originator's Bank to pay $10,000 to the account of Beneficiary in Beneficiary's Bank. Since the amount of Originator's payment order is small, if Originator's Bank and Beneficiary's Bank do not have an account relationship, Originator's Bank may execute Originator's order by issuing a teller's check payable to Beneficiary's Bank for $10,000 along with instructions to credit Beneficiary's account in that amount. The instruction to Beneficiary's Bank to credit Beneficiary's account is a payment order. The check is the means by which Originator's Bank pays its obligation as sender of the payment order. The instruction of Originator's Bank to Beneficiary's Bank might be given in a letter accompanying the check or it may be written on the check itself. In either case the instruction to Beneficiary's Bank is a payment order but the check itself (which is an order to pay addressed to the drawee rather than to Beneficiary's Bank) is an instrument under Article 3 and is not a payment order. The check can be both the means by which Originator's Bank pays its obligation under § 4A-402(b) to Beneficiary's Bank and the means by which the instruction to Beneficiary's Bank is transmitted.

6. Most payments covered by Article 4A are commonly referred to as wire transfers and usually involve some kind of electronic transmission, but the applicability of Article 4A does not depend upon the means used to transmit the instruction of the sender. Transmission may be by letter or other written communication, oral communication or electronic communication. An oral communication is normally given by telephone. Frequently the message is recorded by the receiving bank to provide evidence of the transaction, but apart from problems of proof there is no need to record the oral instruction. Transmission of an instruction may be a direct communication between the sender and the receiving bank or through an intermediary such as an agent of the sender, a communication system such as international cable, or a funds transfer system such as CHIPS, SWIFT or an automated clearing house.

SECTION 4A-201. SECURITY PROCEDURE.

"Security procedure" means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may impose obligations on one or both parties and may require the use of algorithms or other codes, identifying words, ~~or~~ numbers, symbols, sounds or biometrics, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer or reliance on a known email or IP address or phone number is not by itself a security procedure.

Official Comment

A large percentage of payment orders and communications amending or cancelling payment orders are transmitted electronically and it is standard practice to use security procedures that are designed to assure the authenticity of the message through steps designed to ensure the identity of the sender, the integrity of the message, or both. Security procedures can also be used to detect error in the content of messages or to detect payment orders that are transmitted by mistake as in the case of multiple transmission of the same payment order. Security procedures might also apply to communications that are transmitted by telephone or in writing. Section 4A-201 defines these security procedures. The second sentence of the definition provides several examples of a security procedure, but this list is not exhaustive. The inclusion of the phrase "or similar security devices" means that, as new technologies emerge, what can be a security procedure will change. The definition of security procedure limits the term to a procedure "established by agreement of a customer and a receiving bank." The term does not apply to procedures that the receiving bank may follow unilaterally in processing payment orders. The question of whether loss that may result from the transmission of a spurious or erroneous payment order will be borne by the receiving bank or the sender or purported sender is affected by whether a security procedure was or was not in effect and whether there was or was not compliance with the procedure. Security procedures are referred to in Sections 4A-202 and 4A-203, which deal with authorized and verified payment orders, and Section 4A-205, which deals with erroneous payment orders.

Reporter's Note

The proposed amendments to this provision are intended to clarify the definition, not to change its substance.

SECTION 4A-202. AUTHORIZED AND VERIFIED PAYMENT ORDERS.

(a) A payment order received by the receiving bank 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.

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

the security procedure and any ~~written~~ agreement or instruction of the customer, evidenced by a record, 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~~ an agreement evidenced by a record 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.

(c) Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and 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. A security procedure is deemed to be commercially reasonable if (i) the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and (ii) the customer expressly agreed in ~~writing~~ a record to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the bank's obligations under the security procedure chosen by the customer.

(d) The term "sender" in this Article includes the customer in whose name a payment order is issued if the order is the authorized order of the customer under subsection (a), or it is effective as the order of the customer under subsection (b).

(e) This section applies to amendments and cancellations of payment orders to the same extent it applies to payment orders.

(f) Except as provided in this section and in Section 4A-203(a)(1), rights and obligations arising under this section or Section 4A-203 may not be varied by agreement.

Official Comment

This section is discussed in the Comment following Section 4A-203.

SECTION 4A-203. UNENFORCEABILITY OF CERTAIN VERIFIED PAYMENT ORDERS.

(a) If an accepted payment order is not, under Section 4A-202(a), an authorized order of a customer identified as sender, but is effective as an order of the customer pursuant to Section 4A-202(b), the following rules apply:

(1) By express ~~written~~ agreement evidenced by a record, the receiving bank may limit the extent to which it is entitled to enforce or retain payment of the payment order.

(2) The receiving bank is not entitled to enforce or retain payment of the payment order if the customer proves that:

(A) the customer's failure to comply with the customer's obligations under the security procedure was not a material cause of the unauthorized payment order; and

(B) the order was not caused, 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 (ii) who obtained access to transmitting facilities of the customer or 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 access device, computer software, or the like.

(b) This section applies to amendments of payment orders to the same extent it applies to payment orders.

Official Comment

1. Some person will always be identified as the sender of a payment order. Acceptance of the order by the receiving bank is based on a belief by the bank that the order was authorized by the person identified as the sender. If the receiving bank is the beneficiary's bank acceptance means that the receiving bank is obliged to pay the beneficiary. If the receiving bank is not the beneficiary's bank, acceptance means that the receiving bank has executed the sender's order and is obliged to pay the bank that accepted the order issued in execution of the sender's order. In either case the receiving bank may suffer a loss unless it is entitled to enforce payment of the payment order that it accepted. If the person identified as the sender of the order refuses to pay on the ground that the order was not authorized by that person, what are the rights of the receiving bank? In the absence of a statute or agreement that specifically addresses the issue, the question usually will be resolved by the law of agency. In some cases, the law of agency works

well. For example, suppose the receiving bank executes a payment order given by means of a letter apparently written by a corporation that is a customer of the bank and apparently signed by an officer of the corporation. If the receiving bank acts solely on the basis of the letter, the corporation is not bound as the sender of the payment order unless the signature was that of the officer and the officer was authorized to act for the corporation in the issuance of payment orders, or some other agency doctrine such as apparent authority or estoppel causes the corporation to be bound. Estoppel can be illustrated by the following example. Suppose P is aware that A, who is unauthorized to act for P, has fraudulently misrepresented to T that A is authorized to act for P. T believes A and is about to rely on the misrepresentation. If P does not notify T of the true facts although P could easily do so, P may be estopped from denying A's lack of authority. A similar result could follow if the failure to notify T is the result of negligence rather than a deliberate decision. Restatement, Second, Agency § 8B. Other equitable principles such as subrogation or restitution might also allow a receiving bank to recover with respect to an unauthorized payment order that it accepted. In Gatoil (U.S.A.), Inc. v. Forest Hill State Bank, 1 U.C.C. Rep. Serv. 2d 171 (D.Md. 1986), a joint venturer not authorized to order payments from the account of the joint venture, ordered a funds transfer from the account. The transfer paid a bona fide debt of the joint venture. Although the transfer was unauthorized the court refused to require recredit of the account because the joint venture suffered no loss. The result can be rationalized on the basis of subrogation of the receiving bank to the right of the beneficiary of the funds transfer to receive the payment from the joint venture.

But in most cases these legal principles give the receiving bank very little protection in the case of an authorized payment order. Cases like those just discussed are not typical of the way that most payment orders are transmitted and accepted, and such cases are likely to become even less common. Given the large amount of the typical payment order, a prudent receiving bank will be unwilling to accept a payment order unless it has assurance that the order is what it purports to be. This assurance is normally provided by security procedures described in Section 4A-201.

In a very large percentage of cases covered by Article 4A, transmission of the payment order is made electronically. The receiving bank may be required to act on the basis of a message that appears on a computer screen. Common law concepts of authority of agent to bind principal are not helpful. There is no way of determining the identity or the authority of the person who caused the message to be sent. The receiving bank is not relying on the authority of any particular person to act for the purported sender. The case is not comparable to payment of a check by the drawee bank on the basis of a signature that is forged. Rather, the receiving bank relies on a security procedure pursuant to which the authenticity of the message can be "tested" by various devices which are designed to provide certainty that the message is that of the sender identified in the payment order. In the wire transfer business the concept of "authorized" is different from that found in agency law. In that business a payment order is treated as the order of the person in whose name it is issued if it is properly tested pursuant to a security procedure and the order passes the test.

Section 4A-202 reflects the reality of the wire transfer business. A person in whose name a payment order is issued is considered to be the sender of the order if the order is "authorized" as stated in subsection (a) or if the order is "verified" pursuant to a security procedure in

compliance with subsection (b). If subsection (b) does not apply, the question of whether the customer is responsible for the order is determined by the law of agency. The issue is one of actual or apparent authority of the person who caused the order to be issued in the name of the customer. In some cases the law of agency might allow the customer to be bound by an unauthorized order if conduct of the customer can be used to find an estoppel against the customer to deny that the order was unauthorized. If the customer is bound by the order under any of these agency doctrines, subsection (a) treats the order as authorized and thus the customer is deemed to be the sender of the order. In most cases, however, subsection (b) will apply. In that event there is no need to make an agency law analysis to determine authority. Under Section 4A-202, the issue of liability of the purported sender of the payment order will be determined by agency law only if the receiving bank did not comply with subsection (b).

2. The scope of Section 4A-202 can be illustrated by the following cases. Case #1. A payment order purporting to be that of Customer is received by Receiving Bank but the order was fraudulently transmitted by a person who had no authority to act for Customer. Case #2. An authentic payment order was sent by Customer, but before the order was received by Receiving Bank the order was fraudulently altered by an unauthorized person to change the beneficiary. Case #3. An authentic payment order was received by Receiving Bank, but before the order was executed by Receiving Bank a person who had no authority to act for Customer fraudulently sent a communication purporting to amend the order by changing the beneficiary. In each case Receiving Bank acted on the fraudulent communication by accepting the payment order. These cases are all essentially similar and they are treated identically by Section 4A-202. In each case Receiving Bank acted on a communication that it thought was authorized by Customer when in fact the communication was fraudulent. No distinction is made between Case #1 in which Customer took no part at all in the transaction and Case #2 and Case #3 in which an authentic order was fraudulently altered or amended by an unauthorized person. If subsection (b) does not apply, each case is governed by subsection (a). If there are no additional facts on which an estoppel might be found, Customer is not responsible in Case #1 for the fraudulently issued payment order, in Case #2 for the fraudulent alteration or in Case #3 for the fraudulent amendment. Thus, in each case Customer is not liable to pay the order and Receiving Bank takes the loss. The only remedy of Receiving Bank is to seek recovery from the person who received payment as beneficiary of the fraudulent order. If there was verification in compliance with subsection (b), Customer will take the loss unless Section 4A-203 applies.

3. Subsection (b) of Section 4A-202 is based on the assumption that losses due to fraudulent payment orders can best be avoided by the use of commercially reasonable security procedures, and that the use of such procedures should be encouraged. The subsection is designed to protect both the customer and the receiving bank. A receiving bank needs to be able to rely on objective criteria to determine whether it can safely act on a payment order. Employees of the bank can be trained to "test" a payment order according to the various steps specified in the security procedure. The bank is responsible for the acts of these employees. Subsection (b)(ii) requires the bank to prove that it accepted the payment order in good faith and "in compliance with the bank's obligations under the security procedure." If the fraud was not detected because the bank's employee did not perform the acts required by the security procedure, the bank has not complied. Subsection (b)(ii) also requires the bank to prove that it

complied with any agreement or instruction that restricts acceptance of payment orders issued in the name of the customer. If an agreement establishing a security procedure places obligations on both the sender and the receiving bank, the receiving bank need prove only that it complied with the obligations placed on the receiving bank. A customer may want to protect itself by imposing limitations on acceptance of payment orders by the bank. For example, the customer may prohibit the bank from accepting a payment order that is not payable from an authorized account, that exceeds the credit balance in specified accounts of the customer, or that exceeds some other amount. Another limitation may relate to the beneficiary. The customer may provide the bank with a list of authorized beneficiaries and prohibit acceptance of any payment order to a beneficiary not appearing on the list. Such limitations may be incorporated into the security procedure itself or they may be covered by a separate agreement or instruction. In either case, the bank must comply with the limitations if the conditions stated in subsection (b) are met. Normally limitations on acceptance would be incorporated into an agreement between the customer and the receiving bank, but in some cases the instruction might be unilaterally given by the customer. If standing instructions or an agreement state limitations on the ability of the receiving bank to act, provision must be made for later modification of the limitations. Normally this would be done by an agreement that specifies particular procedures to be followed. Thus, subsection (b) states that the receiving bank is not required to follow an instruction that violates ~~a written~~ an agreement evidenced by a record. The receiving bank is not bound by an instruction unless it has adequate notice of it. Subsections (25), (26) and (27) of Section 1-201 apply.

Subsection (b)(i) assures that the interests of the customer will be protected by providing an incentive to a bank to make available to the customer a security procedure that is commercially reasonable. If a commercially reasonable security procedure is not made available to the customer, subsection (b) does not apply. The result is that subsection (a) applies and the bank acts at its peril in accepting a payment order that may be unauthorized. Prudent banking practice may require that security procedures be utilized in virtually all cases except for those in which personal contact between the customer and the bank eliminates the possibility of an unauthorized order. The burden of making available commercially reasonable security procedures is imposed on receiving banks because they generally determine what security procedures can be used and are in the best position to evaluate the efficacy of procedures offered to customers to combat fraud. The burden on the customer is to supervise its employees to assure compliance with the security procedure and to safeguard confidential security information and access to transmitting facilities so that the security procedure cannot be breached.

If a receiving bank and its customer agree to make the technology or service of a third party, for example a cloud service provider, part of the security procedure, the selected technology or service might become unavailable or might fail to perform as expected. In such a situation, it might have been impossible for the customer, the receiving bank, or both to comply with the obligations under security procedure. If the receiving bank is unable to prove compliance with the security procedure for purposes of Section 4A-202 and Section 4A-203, the receiving bank will be unable to treat a payment order as effective against the customer under Section 4A-202(b).

Example: Bank and Customer agree that the authenticity of Customer's payment orders will be verified pursuant to a security procedure that provides that both parties will use

Service Provider's Secure Communication Product. The Secure Communication Product includes an authenticated connection between users and an algorithm that produces a fraud risk score for each payment order sent over the connection. In order to use the Secure Communication Product, Customer and Bank must each individually enter into an agreement with Service Provider. Service Provider is the victim of a cyberattack that compromises the fraud score feature of the Secure Communication Product such that every payment order sent over the connection receives a low fraud risk score. After the attack but before it is discovered, Bank processes a payment order in Customer's name that Customer claims was unauthorized. Whether Bank followed the security procedure is a question of fact. If it is determined that, because the product malfunctioned or otherwise, Bank did not follow the security procedure, Bank will not be able to treat the payment orders as authorized under 4A-202. If instead it is determined that Bank did follow the security procedure, Customer may be able to shift the loss back to Bank. To do so, Customer will need to demonstrate that Customer followed the security procedure (or if Customer did not, that its failure to follow the procedure was not a material cause of the unauthorized order).

4. The principal issue that is likely to arise in litigation involving subsection (b) is whether the security procedure in effect when a fraudulent payment order was accepted was commercially reasonable. In considering this issue, a court will need to consider the totality of the security procedure, including each party's obligations under such procedure. The concept of what is commercially reasonable in a given case is flexible. Verification entails labor and equipment costs that can vary greatly depending upon the degree of security that is sought. A customer that transmits very large numbers of payment orders in very large amounts may desire and may reasonably expect to be provided with state-of-the-art procedures that provide maximum security. But the expense involved may make use of a state-of-the-art procedure infeasible for a customer that normally transmits payment orders infrequently or in relatively low amounts. Another variable is the type of receiving bank. It is reasonable to require large money center banks to make available state-of-the-art security procedures. On the other hand, the same requirement may not be reasonable for a small country bank. A receiving bank might have several security procedures that are designed to meet the varying needs of different customers. The type of payment order is another variable. For example, in a wholesale wire transfer, each payment order is normally transmitted electronically and individually. A testing procedure will be individually applied to each payment order. In funds transfers to be made by means of an automated clearing house many payment orders are incorporated into an electronic device such as a magnetic tape that is physically delivered. Testing of the individual payment orders is not feasible. Thus, a different kind of security procedure must be adopted to take into account the different mode of transmission.

The issue of whether a particular security procedure is commercially reasonable is a question of law. Whether the receiving bank complied with the procedure is a question of fact. It is appropriate to make the finding concerning commercial reasonability a matter of law because security procedures are likely to be standardized in the banking industry and a question of law standard leads to more predictability concerning the level of security that a bank must offer to its customers. The purpose of subsection (b) is to encourage banks to institute

reasonable safeguards against fraud but not to make them insurers against fraud. A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge deciding the question would have opted for a more stringent procedure. For example, the use of a computer program to detect fraud is not commercially unreasonable merely because it does not detect all fraud or because another system or approach might be more successful at detecting fraud. The standard is not whether the security procedure is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank, which is a lower standard. What is reasonable for a particular customer requires the court to consider 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. Article 4A does not create an affirmative obligation on the receiving bank to obtain information about its customer. However, whatever knowledge the bank does have about the customer is relevant in determining the commercial reasonableness of the security procedure. ~~On the other hand, a~~ A security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank and customer should not be held to be commercially reasonable. Subsection (c) states factors to be considered by the judge in making the determination of commercial reasonableness. The reasonableness of a security procedure is to be determined at the time that a payment order is processed, not that the time the customer and the bank agree to the security procedure. Accordingly, a security procedure that was reasonable when agreed to might become unreasonable as technologies emerge, prevailing practices change, or the bank acquires knowledge about the customer. Sometimes an informed customer refuses a security procedure that is commercially reasonable and suitable for that customer and insists on using a higher-risk procedure because it is more convenient or cheaper. In that case, under the last sentence of subsection (c), the customer has voluntarily assumed the risk of failure of the procedure and cannot shift the loss to the bank. But this result follows only if the customer expressly agrees in ~~writing~~ a record to assume that risk. It is implicit in the last sentence of subsection (c) that a bank that accedes to the wishes of its customer in this regard is not acting in bad faith by so doing so long as the customer is made aware of the risk. In all cases, however, a receiving bank cannot get the benefit of subsection (b) unless it has made available to the customer a security procedure that is commercially reasonable and suitable for use by that customer. In most cases, the mutual interest of bank and customer to protect against fraud should lead to agreement to a security procedure which is commercially reasonable.

5. Subsection (b) generally allows a receiving bank to treat a payment order as authorized by the customer if the bank accepts the payment order in good faith and incompliance with the bank's obligations under a commercially reasonable, agreed-upon security procedure. For this purpose, "good faith" requires the exercise of reasonable commercial standards of fair dealing, *see* § 4A-105(a)(6), not the absence of negligence. Consequently, the bank has no duty, beyond that to which the bank has agreed, to investigate suspicious activity or to advise its customer of such activity. However, a bank that obtains knowledge that a customer has not properly secured the customer's operations or knowledge that the customer is the victim of identity fraud might not be acting in good faith if the bank thereafter accepts a payment order [that] [, particularly if the order] significantly departs from the customer's prior practices.

~~5.~~6. The effect of Section 4A-202(b) is to place the risk of loss on the customer if an unauthorized payment order is accepted by the receiving bank after verification by the bank in compliance with a commercially reasonable security procedure. An exception to this result is provided by Section 4A-203(a)(2). The customer may avoid the loss resulting from such a payment order if the customer can prove that the customer's failure to comply with the customer's obligations under the security procedure was not a material cause of the unauthorized payment order and that the fraud was not committed by a person described in that subsection. Breach of a commercially reasonable security procedure requires that the person committing the fraud have knowledge of how the procedure works and knowledge of codes, identifying devices, and the like. That person may also need access to transmitting facilities through an access device or other software in order to breach the security procedure. This confidential information must be obtained either from a source controlled by the customer or from a source controlled by the receiving bank. If the customer can prove that the person committing the fraud did not obtain the confidential information from an agent or former agent of the customer or from a source controlled by the customer and that the customer's failure to comply with the customer's obligations under the security procedure was not a material cause of the unauthorized payment order, the loss is shifted to the bank. "Prove" is defined in Section 4A-105(a)(7). Because of bank regulation requirements, in this kind of case there will always be a criminal investigation as well as an internal investigation of the bank to determine the probable explanation for the breach of security. Because a funds transfer fraud usually will involve a very large amount of money, both the criminal investigation and the internal investigation are likely to be thorough. In some cases there may be an investigation by bank examiners as well. Frequently, these investigations will develop evidence of who is at fault and the cause of the loss. The customer will have access to evidence developed in these investigations and that evidence can be used by the customer in meeting its burden of proof.

~~6.~~ 7. The effect of Section 4A-202(b) may also be changed by an agreement meeting the requirements of Section 4A-203(a)(1). Some customers may be unwilling to take all or part of the risk of loss with respect to unauthorized payment orders even if all of the requirements of Section 4A-202(b) are met. By virtue of Section 4A-203(a)(1), a receiving bank may assume all of the risk of loss with respect to unauthorized payment orders or the customer and bank may agree that losses from unauthorized payment orders are to be divided as provided in the agreement.

~~7.~~8. In a large majority of cases the sender of a payment order is a bank. In many cases in which there is a bank sender, both the sender and the receiving bank will be members of a funds transfer system over which the payment order is transmitted. Since Section 4A-202(f) does not prohibit a funds transfer system rule from varying rights and obligations under Section 4A-202, a rule of the funds transfer system can determine how loss due to an unauthorized payment order from a participating bank to another participating bank is to be allocated. A funds transfer system rule, however, cannot change the rights of a customer that is not a participating bank. § 4A-501(b). Section 4A-202(f) also prevents variation by agreement except to the extent stated.

Reporter's Note

The proposed new comment 5 is offered for discussion purposes only. It is intended to provide a modicum of guidance on when a receiving bank acts "in good faith" in accepting a payment order. The Drafting Committee might conclude, however, that it would be undesirable to step into the thicket of good faith, where small changes in fact can be highly relevant. For example, in referring to "a customer has not properly secured the customer's operations or knowledge that the customer is the victim of identity fraud," the draft comment does not distinguish threats arising from inside the customer's operations from threats arising outside those operation. Yet that distinction might be relevant.

SECTION 4A-206. TRANSMISSION OF PAYMENT ORDER THROUGH FUNDS-TRANSFER OR OTHER COMMUNICATION SYSTEM.

(a) If a payment order addressed to a receiving bank is transmitted to a funds-transfer system or other third-party communication system for transmittal to the bank and transmission through that system is not part of a security procedure agreed to by the sender and the bank, the system is deemed to be an agent of the sender for the purpose of transmitting the payment order to the bank. If there is a discrepancy between the terms of the payment order transmitted to the system and the terms of the payment order transmitted by the system to the bank, the terms of the payment order of the sender are those transmitted by the system. This section does not apply to a funds-transfer system of the Federal Reserve Banks.

(b) This section applies to cancellations and amendments of payment orders to the same extent it applies to payment orders.

Official Comment

1. A payment order may be issued to a receiving bank directly by delivery of a writing or electronic device or by an oral or electronic communication. If an agent of the sender is employed to transmit orders on behalf of the sender, the sender is bound by the order transmitted by the agent on the basis of agency law. Section 4A-206 is an application of that principle to cases in which a funds transfer or communication system acts as an intermediary in transmitting the sender's order to the receiving bank. ~~The~~ In general, the intermediary is deemed to be an agent of the sender for the purpose of transmitting payment orders and related messages for the sender. In such a situation, Section 4A-206 deals with error by the intermediary. However, when transmission through the intermediary is part of an agreed-upon security procedure, the intermediary is the agent of both the sender and the receiving bank, and Section 4A-206 does not apply.

2. Transmission by an automated clearing house of an association of banks other than the Federal Reserve Banks is an example of a transaction covered by Section 4A-206. Suppose Originator orders Originator's Bank to cause a large number of payments to be made to many accounts in banks in various parts of the country. These payment orders are electronically transmitted to Originator's Bank and stored in an electronic device that is held by Originator's Bank. Or, transmission of the various payment orders is made by delivery to Originator's Bank of an electronic device containing the instruction to the bank. In either case the terms of the various payment orders by Originator are determined by the information contained in the electronic device. In order to execute the various orders, the information in the electronic device must be processed. For example, if some of the orders are for payments to accounts in Bank X and some to accounts in Bank Y, Originator's Bank will execute these orders of Originator by issuing a series of payment orders to Bank X covering all payments to accounts in that bank, and by issuing a series of payment orders to Bank Y covering all payments to accounts in that bank. The orders to Bank X may be transmitted together by means of an electronic device, and those to Bank Y may be included in another electronic device. Typically, this processing is done by an automated clearing house acting for a group of banks including Originator's Bank. The automated clearing house is a funds transfer system. Section 4A-105(a)(5). Originator's Bank delivers Originator's electronic device or transmits the information contained in the device to the funds transfer system for processing into payment orders of Originator's Bank to the appropriate beneficiary's banks. The processing may result in an erroneous payment order. Originator's Bank, by use of Originator's electronic device, may have given information to the funds transfer system instructing payment of $100,000 to an account in Bank X, but because of human error or an equipment malfunction the processing may have converted that instruction into an instruction to Bank X to make a payment of $1,000,000. Under Section 4A-206, Originator's Bank issued a payment order for $1,000,000 to Bank X when the erroneous information was sent to Bank X. Originator's Bank is responsible for the error of the automated clearing house. The liability of the funds transfer system that made the error is not governed by Article 4A. It is left to the law of contract, a funds transfer system rule, or other applicable law.

In the hypothetical case just discussed, if the automated clearing house is operated by a Federal Reserve Bank, the analysis is different. Section 4A-206 does not apply. Originator's Bank will execute Originator's payment orders by delivery or transmission of the electronic information to the Federal Reserve Bank for processing. The result is that Originator's Bank has issued payment orders to the Federal Reserve Bank which, in this case, is acting as an intermediary bank. When the Federal Reserve Bank has processed the information given to it by Originator's Bank it will issue payment orders to the various beneficiary's banks. If the processing results in an erroneous payment order, the Federal Reserve Bank has erroneously executed the payment order of Originator's Bank and the case is governed by Section 4A-303.

Reporter's Note

The proposed amendments to this provision and to comment 1 are offered for discussion purposes only. If the Committee chooses to retain these amendments, it might be desirable to include in the comment to § 4A-202 a cross-reference to § 4A-206(1) and comment 1. If the Committee chooses not to retain these amendments, then it will be necessary to revise the proposed changes to the comments following § 4A-203.

SECTION 4A-207. MISDESCRIPTION OF BENEFICIARY.

(a) Subject to subsection (b), if, in a payment order received by the beneficiary's bank, the name, bank account number, or other identification of the beneficiary refers to a nonexistent or unidentifiable person or account, no person has rights as a beneficiary of the order and acceptance of the order cannot occur.

(b) If a payment order received by the beneficiary's bank identifies the beneficiary both by name and by an identifying or bank account number and the name and number identify different persons, the following rules apply:

(1) Except as otherwise provided in subsection (c), if the beneficiary's bank does not know that the name and number refer to different persons, it may rely on the number as the proper identification of the beneficiary of the order. The beneficiary's bank need not determine whether the name and number refer to the same person.

(2) If the beneficiary's bank pays the person identified by name or knows that the name and number identify different persons, no person has rights as beneficiary except the person paid by the beneficiary's bank if that person was entitled to receive payment from the originator of the funds transfer. If no person has rights as beneficiary, acceptance of the order cannot occur.

(c) If (i) a payment order described in subsection (b) is accepted, (ii) the originator's payment order described the beneficiary inconsistently by name and number, and (iii) the beneficiary's bank pays the person identified by number as permitted by subsection (b)(1), the following rules apply:

(1) If the originator is a bank, the originator is obliged to pay its order.

(2) If the originator is not a bank and proves that the person identified by number was not entitled to receive payment from the originator, the originator is not obliged to pay its order unless the originator's bank proves that the originator, before acceptance of the originator's order, had notice that payment of a payment order issued by the originator might be made by the beneficiary's bank on the basis of an identifying or bank account number even if it identifies a person different from the named beneficiary. Proof of notice may be made by any admissible evidence. The originator's bank satisfies the burden of proof if it proves that the originator, before the payment order was accepted, ~~signed a writing~~ authenticated a record stating the information to which the notice relates.

(d) In a case governed by subsection (b)(1), if the beneficiary's bank rightfully pays the person identified by number and that person was not entitled to receive payment from the originator, the amount paid may be recovered from that person to the extent allowed by the law governing mistake and restitution as follows:

(1) If the originator is obliged to pay its payment order as stated in subsection (c), the originator has the right to recover.

(2) If the originator is not a bank and is not obliged to pay its payment order, the originator's bank has the right to recover.

Official Comment

1. Subsection (a) deals with the problem of payment orders issued to the beneficiary's bank for payment to nonexistent or unidentifiable persons or accounts. Since it is not possible in that case for the funds transfer to be completed, subsection (a) states that the order cannot be accepted. Under Section 4A-402(c), a sender of a payment order is not obliged to pay its order unless the beneficiary's bank accepts a payment order instructing payment to the beneficiary of that sender's order. Thus, if the beneficiary of a funds transfer is nonexistent or unidentifiable, each sender in the funds transfer that has paid its payment order is entitled to get its money back.

2. Subsection (b), which takes precedence over subsection (a), deals with the problem of payment orders in which the description of the beneficiary does not allow identification of the beneficiary because the beneficiary is described by name and by an identifying number or an account number and the name and number refer to different persons. A very large percentage of payment orders issued to the beneficiary's bank by another bank are processed by automated means using machines capable of reading orders on standard formats that identify the beneficiary by an identifying number or the number of a bank account. The processing of the order by the beneficiary's bank and the crediting of the beneficiary's account are done by use of the identifying or bank account number without human reading of the payment order itself. The process is comparable to that used in automated payment of checks. The standard format, however, may also allow the inclusion of the name of the beneficiary and other information which can be useful to the beneficiary's bank and the beneficiary but which plays no part in the process of payment. If the beneficiary's bank has both the account number and name of the beneficiary supplied by the originator of the funds transfer, it is possible for the beneficiary's bank to determine whether the name and number refer to the same person, but if a duty to make that determination is imposed on the beneficiary's bank the benefits of automated payment are lost. Manual handling of payment orders is both expensive and subject to human error. If payment orders can be handled on an automated basis there are substantial economies of operation and the possibility of clerical error is reduced. Subsection (b) allows banks to utilize automated processing by allowing banks to act on the basis of the number without regard to the name if the bank does not know that the name and number refer to different persons. "Know" is defined in Section 1-201(25) to mean actual knowledge, and Section 1-201(27) states rules for determining when an organization has knowledge of information received by the organization.

The time of payment is the pertinent time at which knowledge or lack of knowledge must be determined.

Although the clear trend is for beneficiary's banks to process payment orders by automated means, Section 4A-207 is not limited to cases in which processing is done by automated means. A bank that processes by semi-automated means or even manually may rely on number as stated in Section 4A-207.

In cases covered by subsection (b) the erroneous identification would in virtually all cases be the identifying or bank account number. In the typical case the error is made by the originator of the funds transfer. The originator should know the name of the person who is to receive payment and can further identify that person by an address that would normally be known to the originator. It is not unlikely, however, that the originator may not be sure whether the identifying or account number refers to the person the originator intends to pay. Subsection (b)(1) deals with the typical case in which the beneficiary's bank pays on the basis of the account number and is not aware at the time of payment that the named beneficiary is not the holder of the account which was paid. In some cases the false number will be the result of error by the originator. In other cases fraud is involved. For example, Doe is the holder of shares in Mutual Fund. Thief, impersonating Doe, requests redemption of the shares and directs Mutual Fund to wire the redemption proceeds to Doe's account #12345 in Beneficiary's Bank. Mutual Fund originates a funds transfer by issuing a payment order to Originator's Bank to make the payment to Doe's account #12345 in Beneficiary's Bank. Originator's Bank executes the order by issuing a conforming payment order to Beneficiary's Bank which makes payment to account #12345. That account is the account of Roe rather than Doe. Roe might be a person acting in concert with Thief or Roe might be an innocent third party. Assume that Roe is a gem merchant that agreed to sell gems to Thief who agreed to wire the purchase price to Roe's account in Beneficiary's Bank. Roe believed that the credit to Roe's account was a transfer of funds from Thief and released the gems to Thief in good faith in reliance on the payment. The case law is unclear on the responsibility of a beneficiary's bank in carrying out a payment order in which the identification of the beneficiary by name and number is conflicting. See *Securities Fund Services, Inc. v. American National Bank*, 542 F.Supp. 323 (N.D.Ill. 1982) and *Bradford Trust Co. v. Texas American Bank*, 790 F.2d 407 (5th Cir. 1986). Section 4A-207 resolves the issue.

If Beneficiary's Bank did not know about the conflict between the name and number, subsection (b)(1) applies. Beneficiary's Bank has no duty to determine whether there is a conflict and it may rely on the number as the proper identification of the beneficiary of the order. When it accepts the order, it is entitled to payment from Originator's Bank. Section 4A-402(b). On the other hand, if Beneficiary's Bank knew about the conflict between the name and number and nevertheless paid Roe, subsection (b)(2) applies. Under that provision, acceptance of the payment order of Originator's Bank did not occur because there is no beneficiary of that order. Since acceptance did not occur Originator's Bank is not obliged to pay Beneficiary's Bank. Section 4A-402(b). Similarly, Mutual Fund is excused from its obligation to pay Originator's Bank. Section 4A-402(c). Thus, Beneficiary's Bank takes the loss. Its only cause of action is against Thief. Roe is not obliged to return the payment to the beneficiary's bank because Roe received the payment in good faith and for value. Article 4A makes irrelevant the issue of whether Mutual Fund was or was not negligent in issuing its payment order.

3. Normally, subsection (b)(1) will apply to the hypothetical case discussed in Comment 2. Beneficiary's Bank will pay on the basis of the number without knowledge of the conflict. In that case subsection (c) places the loss on either Mutual Fund or Originator's Bank. It is not unfair to assign the loss to Mutual Fund because it is the person who dealt with the impostor and it supplied the wrong account number. It could have avoided the loss if it had not used an account number that it was not sure was that of Doe. Mutual Fund, however, may not have been aware of the risk involved in giving both name and number. Subsection (c) is designed to protect the originator, Mutual Fund, in this case. Under that subsection, the originator is responsible for the inconsistent description of the beneficiary if it had notice that the order might be paid by the beneficiary's bank on the basis of the number. If the originator is a bank, the originator always has that responsibility. The rationale is that any bank should know how payment orders are processed and paid. If the originator is not a bank, the originator's bank must prove that its customer, the originator, had notice. Notice can be proved by any admissible evidence, but the bank can always prove notice by providing the customer with a written statement of the required information and obtaining the customer's signature to the statement. That statement will then apply to any payment order accepted by the bank thereafter. The information need not be supplied more than once.

In the hypothetical case if Originator's Bank made the disclosure stated in the last sentence of subsection (c)(2), Mutual Fund must pay Originator's Bank. Under subsection (d)(1), Mutual Fund has an action to recover from Roe if recovery from Roe is permitted by the law governing mistake and restitution. Under the assumed facts Roe should be entitled to keep the money as a person who took it in good faith and for value since it was taken as payment for the gems. In that case, Mutual Fund's only remedy is against Thief. If Roe was not acting in good faith, Roe has to return the money to Mutual Fund. If Originator's Bank does not prove that Mutual Fund had notice as stated in subsection (c)(2), Mutual Fund is not required to pay Originator's Bank. Thus, the risk of loss falls on Originator's Bank whose remedy is against Roe or Thief as stated above. Subsection (d)(2).

SECTION 4A-208. MISDESCRIPTION OF INTERMEDIARY BANK OR BENEFICIARY'S BANK.

(a) This subsection applies to a payment order identifying an intermediary bank or the beneficiary's bank only by an identifying number.

(1) The receiving bank may rely on the number as the proper identification of the intermediary or beneficiary's bank and need not determine whether the number identifies a bank.

(2) The sender is obliged to compensate the receiving bank for any loss and expenses incurred by the receiving bank as a result of its reliance on the number in executing or attempting to execute the order.

(b) This subsection applies to a payment order identifying an intermediary bank or the beneficiary's bank both by name and an identifying number if the name and number identify different persons.

(1) If the sender is a bank, the receiving bank may rely on the number as the proper identification of the intermediary or beneficiary's bank if the receiving bank, when it executes the sender's order, does not know that the name and number identify different persons. The receiving bank need not determine whether the name and number refer to the same person or whether the number refers to a bank. The sender is obliged to compensate the receiving bank for any loss and expenses incurred by the receiving bank as a result of its reliance on the number in executing or attempting to execute the order.

(2) If the sender is not a bank and the receiving bank proves that the sender, before the payment order was accepted, had notice that the receiving bank might rely on the number as the proper identification of the intermediary or beneficiary's bank even if it identifies a person different from the bank identified by name, the rights and obligations of the sender and the receiving bank are governed by subsection (b)(1), as though the sender were a bank. Proof of notice may be made by any admissible evidence. The receiving bank satisfies the burden of proof if it proves that the sender, before the payment order was accepted, ~~signed a writing~~ authenticated a record stating the information to which the notice relates.

(3) Regardless of whether the sender is a bank, the receiving bank may rely on the name as the proper identification of the intermediary or beneficiary's bank if the receiving

bank, at the time it executes the sender's order, does not know that the name and number identify different persons. The receiving bank need not determine whether the name and number refer to the same person.

(4) If the receiving bank knows that the name and number identify different persons, reliance on either the name or the number in executing the sender's payment order is a breach of the obligation stated in Section 4A-302(a)(1).

Official Comment

1. This section addresses an issue similar to that addressed by Section 4A-207. Because of automation in the processing of payment orders, a payment order may identify the beneficiary's bank or an intermediary bank by an identifying number. The bank identified by number might or might not also be identified by name. The following two cases illustrate Section 4A-208(a) and (b):

Case #1. Originator's payment order to Originator's Bank identifies the beneficiary's bank as Bank A and instructs payment to Account #12345 in that bank. Originator's Bank executes Originator's order by issuing a payment order to Intermediary Bank. In the payment order of Originator's Bank the beneficiary's bank is identified as Bank A but is also identified by number, #67890. The identifying number refers to Bank B rather than Bank A. If processing by Intermediary Bank of the payment order of Originator's Bank is done by automated means, Intermediary Bank, in executing the order, will rely on the identifying number and will issue a payment order to Bank B rather than Bank A. If there is an Account #12345 in Bank B, the payment order of Intermediary Bank would normally be accepted and payment would be made to a person not intended by Originator. In this case, Section 4A-208(b)(1) puts the risk of loss on Originator's Bank. Intermediary Bank may rely on the number #67890 as the proper identification of the beneficiary's bank. Intermediary Bank has properly executed the payment order of Originator's Bank. By using the wrong number to describe the beneficiary's bank, Originator's Bank has improperly executed Originator's payment order because the payment order of Originator's Bank provides for payment to the wrong beneficiary, the holder of Account #12345 in Bank B rather than the holder of Account #12345 in Bank A. Section 4A-302(a) (1) and Section 4A-303(c). Originator's Bank is not entitled to payment from Originator but is required to pay Intermediary Bank. Section 4A-303(c) and Section 4A-402(c). Intermediary Bank is also entitled to compensation for any loss and expenses resulting from the error by Originator's Bank.

If there is no Account #12345 in Bank B, the result is that there is no beneficiary of the payment order issued by Originator's Bank and the funds transfer will not be completed. Originator's Bank is not entitled to payment from Originator and Intermediary Bank is not entitled to payment from Originator's Bank. Section 4A-402(c). Since Originator's Bank improperly executed Originator's payment order it may be liable for damages under Section 4A-

305. As stated above, Intermediary Bank is entitled to compensation for loss and expenses resulting from the error by Originator's Bank.

Case #2. Suppose the same payment order by Originator to Originator's Bank as in Case #1. In executing the payment order Originator's Bank issues a payment order to Intermediary Bank in which the beneficiary's bank is identified only by number, #67890. That number does not refer to Bank A. Rather, it identifies a person that is not a bank. If processing by Intermediary Bank of the payment order of Originator's Bank is done by automated means, Intermediary Bank will rely on the number #67890 to identify the beneficiary's bank. Intermediary Bank has no duty to determine whether the number identifies a bank. The funds transfer cannot be completed in this case because no bank is identified as the beneficiary's bank. Subsection (a) puts the risk of loss on Originator's Bank. Originator's Bank is not entitled to payment from Originator. Section 4A-402(c). Originator's Bank has improperly executed Originator's payment order and may be liable for damages under Section 4A-305. Originator's Bank is obliged to compensate Intermediary Bank for loss and expenses resulting from the error by Originator's Bank.

Subsection (a) also applies if #67890 identifies a bank, but the bank is not Bank A. Intermediary Bank may rely on the number as the proper identification of the beneficiary's bank. If the bank to which Intermediary Bank sends its payment order accepts the order, Intermediary Bank is entitled to payment from Originator's Bank, but Originator's Bank is not entitled to payment from Originator. The analysis is similar to that in Case #1.

2. Subsection (b)(2) of Section 4A-208 addresses cases in which an erroneous identification of a beneficiary's bank or intermediary bank by name and number is made in a payment order of a sender that is not a bank. Suppose Originator issues a payment order to Originator's Bank that instructs that bank to use an intermediary bank identified as Bank A and by an identifying number, #67890. The identifying number refers to Bank B. Originator intended to identify Bank A as intermediary bank. If Originator's Bank relied on the number and issued a payment order to Bank B the rights of Originator's Bank depend upon whether the proof of notice stated in subsection (b)(2) is made by Originator's Bank. If proof is made, Originator's Bank's rights are governed by subsection (b)(1) of Section 4A-208. Originator's Bank is not liable for breach of Section 4A-302(a)(1) and is entitled to compensation from Originator for any loss and expenses resulting from Originator's error. If notice is not proved, Originator's Bank may not rely on the number in executing Originator's payment order. Since Originator's Bank does not get the benefit of subsection (b)(1) in that case, Originator's Bank improperly executed Originator's payment order and is in breach of the obligation stated in Section 4A-302(a)(1). If notice is not given, Originator's Bank can rely on the name if it is not aware of the conflict in name and number. Subsection (b)(3).

3. Although the principal purpose of Section 4A-208 is to accommodate automated processing of payment orders, Section 4A-208 applies regardless of whether processing is done by automation, semi-automated means or manually.