UCC and emerging technologies
Payment systems subgroup
Refined Issues List

As noted going into the January 31, 2020 meeting, Payments System Subgroup feedback was fairly limited with only 16 individuals responding to the survey (and for some questions only 15). The survey results were as follows:

1. Consensus issues (defined to be agreement by all except 1):
    - Address security procedures provisions in 4A
    - Address ISO format issues (do not be specific to any format)
    - Address 3/4 RDC on indemnity issue not covered by Reg CC
2. Significant support but not consensus (defined as 75% agreement):
    - Address 4A for virtual fiat currency (presumption commentary on application of current 4A already)
    - Explore modification of 4A-103 unconditional and smart contracts
    - Clarify definition of bank (while raised as a 4A issue it was noted that this is really a 3/4/4A issue)
    - Add commentary to Article 4 on application of Reg CC
    - Add commentary to Article 4A to address technology (69% support – 11/4 vote)
3. Split views (close to split):
    - Whether to address on-line mobile in 3/4
    - Drafting committee should explore rules for transfer systems that involve nonbank intermediaries – strong support to address the topic but split as to whether to limit work to non-consumer transfers
    - Default rules for non-fiat virtual currency – split (7 yes, 3 only for non-consumer, 5 no)

As a result of the discussions at the Study Committee meeting in January, the issues list was refined.

Decision 1 ISO 20022: There was consensus that the issues around the new ISO message format should be addressed through PEB Commentary and that a draft of that commentary should be presented to the PEB at its next meeting. Stephanie Heller will draft this commentary.

Decision 2 Regulation CC: There was consensus that a PEB Commentary should be drafted that would provide a roadmap of how Regulation CC affects UCC provisions (similar to the commentary in Regulation CC that often refers back to the UCC). While this was viewed as important to ensuring that lawyers who do not often practice in the space are aware of the inter section between Federal and state law, there was also recognition that any such commentary would have to be carefully crafted so as not to become stale with further revisions to Regulation CC and so as not to express legal opinions on the intent of Regulation CC. Pat Fry offered to draft the commentary.

Decision 3 No Further Action: The following topics explored by the Payment Systems Subgroup are not ripe for advancement at this time:

- Article 4A commentary to explain the application of the law when new technologies are used;
- A new Article 4B to address payments that involve nonbank parties (and therefore fall outside of Article 4A); and
- Changes to Part 4 of Article 4 to address the bank/customer relationship in the context of mobile banking.

Decision 4 Potential Action Items: What follows reflects those issues that the Study Committee suggested should remain on its list along with a suggested approach to addressing the issues. The document reflects feedback from the May Study Committee Meeting and subsequent discussions with interested parties.

Issue 1 Writing: At the Study Committee meeting in January, there was consensus that Article 4A should no longer have a writing requirement. In order to make this change, the following statutory provisions would need to be revised to remove the reference to a writing:

Sections 4A-202, 203, 305 – use the phrase "written agreement" or "express written agreement." These provisions could be amended by striking the word writing and adding the phrase "evidenced by a record." Another approach would be to refer to a record of the agreement of the parties. If referred to a drafting committee, the committee would likely look to other UCC Articles to align with the approach taken in those Articles when the term writing was replaced by the concept of record.

4A-207 (misdescription of beneficiary) and 4A-208 (misdescription of intermediary bank or beneficiary's bank) -- These provisions of Article 4A use the phrase "signed a writing" to provide a safe harbor to be used by an originator's bank or a receiving bank to satisfy the burden of proof established in the provisions. The drafting committee will need to decide whether it is necessary to revise these two provisions given that the existence of a signed writing is not the exclusive means by which a bank can meet its burden of proof. If the drafting committee were to revise these provisions it will want to replace the notion of a signed writing with a record that has been authenticated by the originator or sender respectively.

4A-103, 210 and 211 – use the phrase "orally, electronically, or in writing" to describe what qualifies as a payment order, a notice of rejection, and a communication of cancellation or amendment. Given the manner in which the term "writing" is used in these provisions, it may not be necessary to revise these provisions, but if they were to be revised the drafting committee would simply replace the word "writing" with the word "record."

Issue 2 Security Procedures: In addition to addressing the writing requirement, there was support for exploring modifications to 4A-201 through 4A-204 on security procedures and its related commentary to address the definition of security procedure in light of emerging technologies and the impact of new technologies on the risk allocation scheme in Article 4A. These issues are described in more detail below.

Definition of Security Procedure: Section 4A-201 defines the term security procedure and provides in part that a security procedure "may require use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature of the customer is not by itself a security procedure." A drafting committee may want to consider whether current technologies fit into the definition of security procedure. Is the use of biometrics a "similar security device"? Are all forms of AI properly viewed as an algorithm? Are smart contracts used for authentication either of the two? Given the use of the phrase "or similar security device", there is likely no need to revise the statute to answer these questions. In fact, use of commentary might be preferable as it could make the point that the definition is meant to evolve as technologies and practices evolve.

A second question for a Drafting Committee is whether reliance on a known IP address can be a security procedure or is it more akin to a signature? At least one court has found that an email address alone would be not qualify as a security procedure because it is like a signature. While commentary could be used to address this point, unlike the definition of security procedure which contains a catchall phrase that can be explored in commentary, the carve-out from the definition of security procedure for signatures is specific to the term signature and may not lend itself to a broader interpretation. Therefore this may be best addressed through a statutory change.

If a Drafting Committee were to revise Section 4A-201, it would be useful to clarify that security procedures can include obligations on both parties. This is important for determining liability under 4A-202 and 203. It would also be good to clarify that compliance programs carried out by a receiving bank, such as AML programs, are not part of a security procedure unless the compliance program is included in the agreed upon procedures. This later point can be addressed in commentary.

§ 4A-201: Security Procedures

"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, encryption, callback procedures, or similar security devices. Comparison of 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. Security procedures authenticating a message may include steps to authenticate the identity of the sender as well as to authenticate the integrity of the message. 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 definition provides examples of processes that may be features of a security procedure, such as algorithms and encryption, but this list is not exhaustive. The inclusion of the phrase "or similar security devices" means that as new technologies emerge and security practices evolve, what may be used as part of a security procedure will change. For example, since the passage of Article 4A, the use of biometrics as part of security procedures is now possible as is the use of technology that can enforce certain contractual terms agreed to in a security procedure. The 20XX amendments to this provision clarify the definition but are not intended to change its substance.

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

Allocation of Liability: There are several issues that a drafting committee might want to explore in Sections 4A-202 and 203 that related to the allocation of losses due to an unauthorized payment order. Most of the issues are only indirectly tied to technological changes and several are suggested to address current ambiguity in the law. Given the importance of this issue, however, we have presented the broader proposal below, some of which can be accomplished through commentary and some of which would require changes to the statute.

Article 4A-202 and 203 were carefully crafted to place the risk of unauthorized transfers on the party best positioned to prevent such risk and on the receiving bank where the risk is not reasonably prevented by either party. A drafting committee might want to consider whether additional guidance is needed in light of new data rich payment order formats, heightened supervisory expectations around AML and fraud that are driving the banking industry to expand their compliance efforts beyond traditional payments data, advances in technology that may be able to support real-time fraud detection for institutions that can afford to implement the technology (e.g., AI?), Assuming a similar policy objective continues to exist, how should Article 4A treat these developments when considering what is commercially reasonable and what is good faith. (4A-202 defines "commercially reasonable" in part by reference to "security

procedures in general use by customers and receiving banks similarly situated." Depending on the view of the drafting committee there may be a need for statutory changes or changes to commentary may suffice.

4A-202 requires among other things that a receiving bank prove that it complied with an agreed upon security procedure. Commentary to 4A-203 explains that the burden placed on a receiving bank is to make available a commercially reasonable security procedure while the burden placed on the sender is to supervise its employees and to assure compliance with the procedure. One policy decision that the study committee may wish to address is the allocation of losses in cases where a shared third-party service provider, such as a cloud provider, fails to perform obligations under a security procedure. In such a case, neither the sender nor the receiving bank will be able to demonstrate that it met its obligations. As Article 4A's loss allocation regime is currently formulated, this likely means that a bank will be unable to treat the payment order as effective (and thus would bear losses associated with any unauthorized transfers); however, the interplay between section 4A-202, 4A-206 (dealing with transmissions through communication systems), and agency law, leaves ambiguity that might need to be addressed by a trier of facts and could be aided by commentary.

A separate policy decision arises with respect to the proper treatments of a customer's failure to perform its obligations under an agreement adopting a security procedure. Section 4A-203 and its commentary adequately captures the types of obligations that could arise for a customer today, for example a requirement in a security procedure that the customer implement dual authorization controls or pre-transaction fraud scoring. We have drafted a strawman approach to this issue in proposed changes to § 4A-203.

Among other considerations, the study committee should consider whether the liability regime outlined below is the proper one, the extent to which the ambiguity with respect to shared-service providers should be further addressed, and the extent to which knowledge by the parties should be a factor.

§ 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 its obligations under the security procedure and any ~~written~~ agreement evidenced by a record or instruction of the customer restricting acceptance of payment orders issued in the name of the customer. The bank is not required to follow an instruction that violates an ~~written~~ agreement with the customer evidenced by a record 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 a record~~writing~~ to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the obligations imposed on the bank under the agreement establishing the security procedure chosen by the customer.

* * *

§ 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 in 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 the order was not caused, directly or indirectly, by each of the following: ~~a person~~ (i) a person entrusted at any time with duties to act for the customer with respect to payment orders or the security procedure, ~~or~~ (ii) a person 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, and (iii) the customer's failure to comply with ~~reasonable~~ obligations imposed on it under the agreement establishing the security procedure where the customer's failure was a material cause of the unauthorized payment order. 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 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. Where a security procedure agreement places obligations on both the sender and the receiving bank, the receiving bank need only prove that it complied with the obligations placed on the receiving bank. A customer may separately 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 an express ~~written~~ agreement evidenced in 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.

Where a receiving bank and its customer agree that a third party's technology or service, for example a cloud service provider, is part of the agreed upon security procedure, it is possible that the selected technology or service is unavailable or fails to perform as expected. In such situations it may have been impossible for both the sender and its receiving bank to comply with the security procedure. Consequently, each may be unable to prove compliance with the security procedure for purposes of Section 4A-202 and Section 4A-203, and a receiving bank will be unable to treat a payment order as effective against the customer under Section 4A-202(b). Based on the facts and circumstances, however, a fact finder might conclude that the payment order was authorized under Section 4A-202(a) if the third party providing the technology or service was an agent of the sender as described in Section 4A-206 and there was a discrepancy in the payment order the receiving bank received as described in that section.

[As an 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 a model that produces a fraud 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 comprises the fraud score feature of the Secure Communication Product such that every payment order sent over the connection receives a low fraud risk score. During the attack Bank processes a series of payment orders in Customer's name that Customer claims were unauthorized. The fact of the cyberattack and malfunction of the fraud scoring model is discovered while investigating the Customer's claim that the payment orders were unauthorized. Whether Bank followed the security procedure is a question of fact. The Bank used the required product but the product was not functioning. If it is determined that because the product malfunctioned the Bank did not follow the security procedure, Bank will not be able to treat the payment orders as verified under 4A-202. If instead it is determined that Bank followed the security procedure, Customer may be able to shift the loss back to Bank but it too will need to demonstrate that it followed the security procedure (or if it did not, that its failure to follow the procedure was not a material cause of the unauthorized order). Because the Secure Communication Product is a "communication system," if Bank is responsible for losses based on 4A-202 and 203, Bank may try to shift the loss to Customer under 4A-206. In this example, it is unlikely that Bank will be successful given that there was no discrepancy in the payment 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 ~~it will be important to look at t~~he totality of the security procedure, including both parties' 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 simply because it did not catch all frauds even if another system or approach might have been 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, if a bank has knowledge of the customer, including with respect to its information security posture, a court will consider that knowledge when assessing the commercial reasonableness of the security procedure.

{NOTE TO STUDY COMMITTEE – Since 2005 when the FFIEC first issued its guidance on wholesale transfers to banks with respect to authentication in an internet banking environment, courts have looked to the guidance as a possible proxy for what the industry standard is with respect to its analysis of whether a security procedure is commercially reasonable. The initial guidance in 2005 drew a clear distinction between what constitutes method s of authentication and other aspects of a bank's information security program. In 2011, the FFIEC issued a supplement to the 2005 guidance which has also been cited to by courts. The 2011 guidance blurs the lines between authentication techniques and other actions that a bank may be able to take to limit fraud. The below commentary is written with this backdrop. If this is something that the Study Committee wishes to send forward to a drafting committee to consider, it may be helpful to also provide the FFIEC Guidance and the cases that cite the Guidance. This Guidance is now incorporated in examination handbooks and changes are not subject to a public rule-making process.]

~~On the other hand, a~~A security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank should not be held to be commercially reasonable. Importantly, the prevailing information security practices of similarly situated banks generally, as opposed to the specific prevailing standards for authenticating a message ~~sender,~~ is not part of the commercially reasonable analysis. Subsection (c) states factors to be considered by the judge in making the determination of commercial reasonableness.

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 a record~~writing~~ 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. 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 fraud was not committed ~~by a person~~as 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 a material cause of the ~~person committing the~~ fraud was not ~~otherwise able to commit the fraud due to~~ the customer's failure to comply with the security procedure, 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. 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. 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.

Good faith: Section 4A-202(b) requires a bank to act in good faith in accepting a payment order in order for the bank to treat the payment order as effective against its customer. Under § 4A-105(a)(6) "Good faith" means honesty in fact and the observance of reasonable commercial standards of fair dealing.

Since 2008 when a fraudster sought to initiate nearly $1 billon of unauthorized funds transfers on behalf of the Bank of Bangladesh, there has been increased pressure from the supervisory community to have funds transfer systems obtain visibility into the virtual and physical security of their bank participants' funds transfer operations. In turn, certain funds transfer system operators are making this information available to banks on the system to varying degrees. If a bank obtains knowledge that a sender may not be adequately monitoring its people or securing

its operations, can such bank accept a payment order in good faith from that sender? It would be helpful to have Article 4A commentary that addresses this issue. Because there may be policy arguments on both sides, this issue would benefit from discussions of a drafting committee.

In addition, courts applying 4A-202's good faith acceptance requirement have tended to apply a negligence standard notwithstanding the definition in Article 4A. Sometimes in considering the question of "good faith" acceptance, courts have also turned to the FFIEC Guidance described above. Including commentary that could help focus the court away from negligence should also be considered even though it is not directly tied to technology changes.

Issue 3 Virtual Currency: No decision was made at the January Study Committee meeting on whether the UCC should be revised to support nonfiat virtual currency. Instead it was recognized that more discussion was needed across several dimensions. At the May meeting, a proposal was submitted to limit the UCC's treatment of nonfiat virtual currency to issues arising under Article 9 and generally to look to Article 8 for support for nonfiat virtual currencies that are account based. It was suggested that additional thought might be needed to support the transfer of nonfiat virtual currency for non-intermediated transfers. No decision was made as to whether to pursue this direction though it was noted that understanding the characteristics/rules of specific virtual currency systems might be important if the study committee were to pursue this.

In contrast to the discussions on nonfiat virtual currency, there was strong support of the Payment Systems Subgroup and at the January Study Committee meeting to recommend that a drafting committee add commentary to Articles 3, 4 and 4A to address how the current provisions of those Articles would work if an instrument or a payment order directs payment in a fiat virtual currency. The below discussion focuses on this aspect of virtual currency.

Definition of Money: Money is defined in Article 1 as a medium of exchange authorized or adopted by a domestic or foreign government. While some have asked whether the phrase "medium of exchange" somehow limits the term money to hard currency and coin, there is no reason to read such limitation into the phrase and in several other contexts the term virtual currency has already been defined as a medium of exchange. If this is true, then it is only a matter of time before there is a form of virtual currency in existence that is "money" for purposes of the UCC as there are several foreign governments that appear to be on the verge of adopting a virtual currency in lieu of issuing paper notes and coins.

1-201(a) (24) "Money" means a medium of exchange currently authorized or adopted by a domestic or foreign government. The term includes a monetary unit of account established by an intergovernmental organization or by agreement between two or more countries.

24. "Money." Substantively identical to former Section 1-201. The test is that of sanction of government, whether by authorization before issue or adoption afterward, which recognizes the circulating medium as a part of the official currency of that government. The narrow view that money is limited to legal tender is rejected.

Use of the Term Money in the Payment Articles: The Payments System Subgroup has done an initial review of the payment articles of the UCC and believes that the Articles do not need to be revised even if a government were to authorize or adopt a virtual currency. This preliminary conclusion is based on the ways in which the term "money" is used in these Articles. Specifically, the term money is used in the definition of negotiable instrument and payment order as a limiting factor – to be a negotiable instrument or payment order the instrument or order must be denominated in money. For those instruments and payment orders denominated in virtual currency money and therefore are subject to Articles 3, 4 and 4A, our preliminary analysis suggests that is no problem because engaging in transactions involving instruments or funds transfers is optional:

Article 3 – A person is not required to accept an instrument in satisfaction of an obligation or accept a transfer of an instrument. If a person takes an instrument denominated in a virtual currency that satisfies the definition of money, then the rules of Article 3, including the effect of the instrument on the obligation for which it was taken, instruments payable in foreign money, and discharge, will apply.

Article 4 – As is currently the case, a bank can decide whether to "handle for collection" specific types of items including items denominated in foreign money. A bank is also generally free to set the terms of its accounts and whether to permit its customers to issue checks drawn on those accounts. Some states require banks to offer "minimum" service dollar denominated accounts. If the U.S. Government were to issue virtual currency it is possible that banks might be required to offer accounts denominated in such virtual currency under laws other than Article 4 but Article 4 does not contain such a requirement.

Article 4A – An originator's bank and each intermediary bank may reject any payment order unless the bank has agreed in advance that it will accept such payment order. A beneficiary's bank can also reject a payment order except that acceptance is automatic when the sender is a bank and the beneficiary's bank is paid "the amount of the order" by credit to an account at a bank, credit to its Federal Reserve account, or through a funds transfer system. Presumably, if the beneficiary bank is paid the amount of the order in virtual currency, the beneficiary's bank is able to handle virtual currency. As discussed further below, however, the beneficiary's bank can control for this by contract with its direct senders or by choosing not to participate in a funds transfer system that uses virtual currency as a settlement asset.

Finally, it is helpful to consider how the introduction of virtual currency could affect these Articles. Generally these UCC Articles address the following topics:

- The issuance of an instrument or origination of a payment order – the birth (wholly optional)
- how an instrument is transferred or collected or how a payment order is executed – in other words the mechanics of moving the information from party to party
- how risks are allocated among the parties
- who has an obligation to pay, when the obligation arises, and when it is due
- how an obligation to pay may be settled

The question of virtual currency really only arises in connection with the settlement of an obligation to pay. If the obligation to pay can only be satisfied in virtual currency, then a person must be able to determine before becoming obligated to pay whether it has the ability to make the payment in virtual currency. This should be able to be addressed by contract under all three Articles.

One option that the Study Committee might want to send forward to a drafting committee is whether to include a provision in these articles that would permit a payment obligation denominated in a virtual currency to be satisfied by converting the amount into dollars similar to the provision in Article 3 that addresses foreign money (§3-107). Presumably this provision will

apply to instruments if a foreign government adopts a virtual currency. There is no similar concept in Article 4A. With respect to a virtual currency adopted by the United States, it should suffice to have commentary that makes clear that absent express agreement to the contrary, payment in dollars in any form (credit to a traditional dollar denominated account, dollar denominated virtual currency account or ledger position, or hard currency would all satisfy the obligation).

§ 3-107. INSTRUMENT PAYABLE IN FOREIGN MONEY

Unless the instrument otherwise provides, an instrument that states the amount payable in foreign money may be paid in the foreign money or in an equivalent amount in dollars calculated by using the current bank-offered spot rate at the place of payment for the purchase of dollars on the day on which the instrument is paid.

OFFICIAL COMMENT

The definition of instrument in Section 3-104 requires that the promise or order be payable in "money." That term is defined in Section 1-201(24) and is not limited to United States dollars. Section 3-107 states than an instrument payable in foreign money may be paid in dollars if the instrument does not prohibit it. It also states a conversion rate which applies in the absence of a different conversion rate stated in the instrument. The reference in former Section 3-107(1) to instruments payable in "currency" or "current funds" has been dropped as superfluous.

Issue 4 Unconditional Promise: To qualify as a payment order under Article 4A the instruction cannot state a condition to payment to the beneficiary other than time of payment (note that the amount of a payment order can be fixed or determinable). See 4A-103. The use of "smart contracts" in the payments space may create some questions as to whether there is an unconditional promise to pay. For example, if a trading platform leverages smart contracts to ensure that a payment to a beneficiary is only made if certain actions happen first, is there a conditional payment order? If there are circumstances under which the use of smart contracts could be viewed as creating an instruction that contains a condition to payment, then absent a change to Article 4A (or at least new commentary), the universe of payments that today would fall under Article 4A may be reduced even when as a policy matter the drafters might have wanted those payments to remain within Article 4A. (This same issue did not arise for Articles 3/4 solely because the Subgroup was not tasked with considering electronic instruments (which is where the use of smart contracts could arise).

While not a consensus, there was strong support of the Payment Systems Subgroup and of the participants at the Study Committee meeting to continue to explore this issue. One factual point that may not have been clear during the Study Committee meeting but that may help to explain why this is a potential issue is the fact that Article 4A only addresses credit transfers – the party wanting to make the payment must initiate the instruction, and cannot place a condition on payment to the beneficiary other than time of payment.

We have suggested additional commentary below that focuses on the use of agency and is not dependent on any particular type of technology. We believe the proposed commentary could help to clarify the treatment of smart contracts. As seemingly required by Article 4A, however, the example includes the initiation of a payment order by the agent after the hypothetical condition is resolved. To the extent that smart contracting practices do not accommodate the issuance of a payment order, then it may be necessary to revise the statutory text if the Study Committee wants these payments to be covered by Article 4A.

§ 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.

…

OFFICIAL COMMENT

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

§ 4A-104. Funds Transfer--Definitions

…

OFFICIAL COMMENT

…

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, 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 of the New York bank 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.

In the example above, the New York bank's instruction was conditional because the instruction it gave the California bank as a prospective receiving bank included a

condition to payment of the beneficiary. On the other hand, if the condition could be resolved prior to the initiation of the payment order, then Article 4A would apply. As an example, X and its securities broker have agreed that X will buy securities at certain prices. X uses New York bank and its securities broker uses California bank and X has authorized its bank to follow instructions issued in X's name by an application used by the securities broker to initiate trades; in essence the application is the agent of X. Securities broker's application monitors the prices of the relevant securities. If securities broker's application determines a security reaches X's purchase price, the application instructs New York bank to pay securities broker the amount of the purchase price. The instruction will state no condition.

Issue 5 Bank: There was support of the Payment Systems Subgroup and at the Study Committee meeting to continue to explore whether the definition of "bank" needs to be refined in light of the emergence of fintech and other financial institutions. The current definition in combination with its related commentary leaves open the possibility that various types of institutions that engage in transfers on behalf of customers could be considered banks for purposes of Article 4A. Implicit in the question of the proper scoping of an Article 4A bank is the consideration of what types of institutions should be expected to take on the obligations under Article 4A, what types of institutions should benefit from any related protections, and whether these are reserved for institutions that are regulated and supervised and if so does the type of supervision and regulation matter?.

In a recent example of this issue, the Illinois Supreme Court determined that a futures commission merchant (FCM) is a bank for Article 4A purposes because it regularly assisted customers in conducting funds transfers, even though the FCM did so by instructing a bank that held one or more segregated customer deposit accounts for the benefit of such customers. Organizations like these may be better characterized as agents for their customers; not Article 4A receiving banks. From an emerging technology standpoint, the definition may be more important as new technology enables different organizations to enter the space. One example of such an entity would be a future entity authorized by the OCC under its "fintech" charter, a charter that is expressly premised on the entity making loans and/or payments but not being in the business of taking deposits.

Whether this issue ultimately moves forward may depend in part on whether the issue is sufficiently tied to emerging technology as well as the Study Committee's views on the risk of unintended consequences of clarifying the definition or leaving it as is. One way to create such clarity would be to identify a bank as an institution that is engaged in the business of receiving deposits, which would include institutions engaged in an activity in which only banks may engage.

If it is advanced, we believe the change might need to be to statutory language but at a minimum would require changes to the commentary and may require alignment with Article 4.

§ 4-105. Definitions of Types of Banks.

(1) ["Bank" means a person engaged in the business of banking, including a savings bank, savings and loan association, credit union, or trust company;]

Official Comment

2. Paragraph (1): "Bank" is defined in Section 1-201(4) as meaning "any person engaged in the business of banking." The definition in paragraph (1) makes clear that "bank" includes savings banks, savings and loan associations, credit unions and trust companies, in addition to the commercial banks commonly denoted by use of the term "bank."

§ 4A-105. Other Definitions.

…

(2) "Bank" means a person engaged in the business of receiving depositsbanking and includes a savings bank, savings and loan association, credit union, and trust company. A branch or separate office of a bank is a separate bank for purposes of this Article.

Official Comment

1. The definition of "bank" in subsection (a)(2) includes all some institutions that are not commercial banks authorized under applicable law to engage in the business of receiving deposits. The definition reflects the fact that many forms of deposit-takingfinancial institutions now perform functions previously restricted to commercial banks, including acting on behalf of customers in funds transfers. Since many funds transfers involve payment orders to or from foreign countries the definition also covers foreign banks. The definition also includes Federal Reserve Banks. Funds transfers carried out by Federal Reserve Banks are described in Comments 1 and 2 to Section 4A-107.

Issue 6 Remote Deposit Capture: There was consensus that the issues (discussed more below) that arise in the context of remote deposit capture and that are not answered by Regulation CC should be pursued. However there was a request to see whether the Board of Governors might be willing to at least advance the indemnity issue in light of the fact that Regulation CC already contemplates remote deposit capture and Articles 3 and 4 do not. Board staff has indicated that the issue was added to a list of possible future revisions but that there is no near term effort to revise Regulation CC.

Indemnity: Under Regulation CC if a payee remotely deposits a check and then deposits the original paper check a second time with a different bank, if the paper check is returned and the depositary bank cannot charge back the payee's account, the depositary bank would have a warranty claim against the bank that accepted the remote deposit (the "truncating bank"). Regulation CC does not address the situation where the second deposit is done not by the payee but by a holder in due course (HDC) like a check casher. In such a situation, when the check is returned to the depositary bank, the depositary bank will charge back the HDC. The HDC will not be able to pursue a claim based on Regulation CC's remote deposit capture indemnity but may be able to bring a claim on the instrument against the drawer. It is not clear that the drawer would have a defense to payment or a claim against the truncating bank. Is this the right policy outcome or should the UCC be revised to include an indemnity by the truncating bank under certain circumstances (e.g., there was no RDC restrictive endorsement on the original check)?

Since the May meeting of the Study Committee several observers have indicated that it may be premature to revise Article 3 in this way given that the Regulation CC indemnity is still fairly new and is viewed by the industry as introducing uncertainty as to its application. It was suggested that it would be better to rely on the remedies currently available to protect the HDC, namely a claim against the drawer. It was further suggested that the drawer would have a breach of warranty claim under Regulation CC against each bank that transferred or presented the "electronic check" because the drawer was forced to pay the check twice."[1]

[1] (a) Warranties with respect to electronic checks and electronic returned checks. (1) Each bank that transfers or presents an electronic check or electronic returned check and receives a settlement or other consideration for it warrants that—

(i) The electronic image accurately represents all of the information on the front and back of the original check as of the time that the original check was truncated and the electronic information includes an accurate record of all MICR line information required for a substitute check under §229.2(aaa) and the amount of the check, and

(ii) No person will receive a transfer, presentment, or return of, or otherwise be charged for an electronic check or electronic returned check, the original check, a substitute check, or a paper or electronic representation of a substitute check such that the person will be asked to make payment based on a check it has already paid.

(2) Each bank that makes the warranties under paragraph (a)(1) of this section makes the warranties to—

(i) In the case of transfers for collection or presentment, the transferee bank, any subsequent collecting bank, the paying bank, and the drawer; and

(ii) In the case of transfers for return, the transferee returning bank, any subsequent returning bank, the depositary bank, and the owner.

§ 3-416. TRANSFER WARRANTIES AND INDEMNITIES

(a) A person who transfers an instrument for consideration warrants to the transferee and, if the transfer is by indorsement, to any subsequent transferee that:
(1) the warrantor is a person entitled to enforce the instrument;
(2) all signatures on the instrument are authentic and authorized;
(3) the instrument has not been altered;
(4) the instrument is not subject to a defense or claim in recoupment of any party which can be asserted against the warrantor;
(5) the warrantor has no knowledge of any insolvency proceeding commenced with respect to the maker or acceptor or, in the case of an unaccepted draft, the drawer; and
(6) with respect to a remotely-created consumer item, that the person on whose account the item is drawn authorized the issuance of the item in the amount for which the item is drawn.

(b) A person to whom the warranties under subsection (a) are made and who took the instrument 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, but not more than the amount of the instrument plus expenses and loss of interest incurred as a result of the breach.

(c) Remote deposit capture indemnity. (1) The indemnity described in paragraph (c)(2) of this section is provided by a depositary bank that—
(i) accepts deposit of an electronic image or other electronic information related to a check;
(ii) Does not receive the check;
(iii) Receives settlement or other consideration for an electronic check or substitute check related to the check; and
(iv) Does not receive a return of an electronic check or substitute check related to the check unpaid.
(2) A depositary bank described in paragraph (c)(1) of this section shall indemnify a person other than the named payee on the check that deposits the check with a depositary bank ~~provides consideration for the check~~ for losses incurred by that person if the loss is due to an electronic check or substitute check related to the check having already been paid.
(3) A person may not make an indemnity claim under paragraph (c)(2) of this section if the check it accepted bore a restrictive indorsement indicating that an electronic image or other electronic information related to the check was deposited.
(d) Indemnity amounts. (1) The amount of the indemnity in paragraphs (c)(2) of this section shall not exceed the sum of—
(i) The amount of the loss of the indemnified person, up to the amount of the settlement or other consideration received by the indemnifying bank; and
(ii) Interest and expenses of the indemnified person (including costs and reasonable attorney's fees and other expenses of representation).

(2)(i) If a loss described in paragraph (c)(2) of this section results in whole or in part from the indemnified person's negligence or failure to act in good faith, then the indemnity amount described in paragraph (d)(1) of this section shall be reduced in proportion to the amount of negligence or bad faith attributable to the indemnified person.

(~~c~~e) The warranties and indemnity stated in subsection (a) and (c) cannot be disclaimed with respect to checks. Unless notice of a claim for breach of warranty or for indemnity is given to the warrantor or indemnitor within 30 days after the claimant has reason to know of the breach or the facts and circumstances giving rise to the indemnity and the identity of the warrantor or indemnitor, the liability of the warrantor or indemnitor under subsections (b) and (d) is discharged to the extent of any loss caused by the delay in giving notice of the claim.

(~~d~~f) A [cause of action] for breach of warranty or indemnity under this section accrues when the claimant has reason to know of the breach or the facts and circumstances giving rise to the indemnity.

This addition would also need to be supplemented with additional definitions that define electronic check and substitute check. Use of other Regulation CC definitions such as "original check" or "truncating bank" could also be helpful.

Lost Instrument: Is there a need to have Article 3 of the UCC address a situation where a check is deposited remotely and destroyed by the depositor and the depositor later determines that the remote deposit was never received by the depositary bank? Will the depositor be able to pursue a claim under UCC 3-309 and does the plain language of 3-309 provide for such a claim under these facts – the image disappears at some point prior to reaching the depositary bank and the original check is purposefully destroyed.

The commentary to Section 3-309 as currently drafted considered the loss of an instrument while in transit. It could be expanded to say that 3-309 is also available if it is an electronic transmission of the instrument that is lost and the instrument itself was destroyed.

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.

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. For similar reasons, the protection of subsection (a) should also be available when an instrument is intentionally destroyed in connection with a remote deposit and capture arrangement, and subsequent to its destruction it is discovered that the image or other electronic information sent for deposit was lost prior to reaching the depositary bank. 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.

Discharge: Is it possible that the intentional destruction of the original check might be treated as discharge under 3-604?

§ 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.

***

To address the concern, we believe that the study committee should consider commentary that to § 3-604 indicating that the intentional voluntary act of destroying a check after using a remote deposit capture service is not an act of discharge (whether or not required under the terms of the RDC service) because there is no intent to discharge under those circumstances.

Issuance and delivery: Since the last meeting of the Study Committee a new issue with respect to current technology has arisen in the context of checks and remote deposit capture services. Since RDC was introduced, vendors have emerged that offer parties to a transaction the ability to make and accept payment by having the payer write a check including signing it, taking a picture of the check using an application on their mobile device and sending the picture to the app vendor in a way that allows the payee (or the vendor acting on behalf of the payee) to then deposit the check through an RDC arrangement with the payee's depositary bank. The original paper check remains in the possession of the drawer. The vendor that provides the mobile app technology is not working with the depositary bank.

An example of such a product currently in use is a mobile app that enables residents to pay their rent by "check." Landlord instructs its tenants (the payer) to download a specific app to their mobile device, and to draw a paper check payable to the landlord in the designated amount, and

date and sign the paper check. The payer then takes a picture of the front and back of the check using the mobile app and the app vendor receives the images and creates an image file on behalf of the landlord. The vendor then transmits that image file to the landlord's bank for deposit through the depositary bank's remote deposit capture service. Another example of a similar non-bank mobile app offering is for home buyers to use in paying earnest money to title companies pending closing.

The question arises as to what type of transaction this is under Article 3 under current law and whether current law should be revised to achieve a different outcome or clarified through commentary to reinforce the current outcome. When considering this question it is important to keep in mind that a depositary bank receiving the images through its remote deposit capture service will likely not be able to determine whether the paper check was in the possession of the payee (their deposit customer) at the time of deposit. Also, if the depositary bank receives the images through its remote deposit capture services, the depositary bank will automatically handle the transactions as check deposits for processing, clearing and settlement, and for handling claims. The definitions in Regulation CC of "electronic check" and "electronically-created item" are also relevant to this discussion. The below analysis is intended to aid discussion.

Under Article 3, the term instrument means a negotiable instrument and a negotiable instrument is either a promise or order, both of which are defined to be writings. Therefore, as currently drafted for a check to be issued it requires the physical movement of the original paper check from the drawer to the payee. In this case, although the check is written and signed by the drawer, the check is never issued (the paper check remains in the drawer's possession), and neither the payee nor the payee's third party processor receives the paper check. Moreover, this is not a remotely created check as it in fact bears the handwritten signature of the drawer.

§ 3-105. ISSUE OF INSTRUMENT.

(a) "Issue" means the first delivery 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.

§ 1-201. General Definitions.
(b)(15) "Delivery", with respect to an instrument, document of title, or chattel paper, means voluntary transfer of possession.

§ 3-103. DEFINITIONS.

(a)(16) "Remotely-created consumer item" means an item drawn on a consumer account, which is not created by the payor bank and does not bear a handwritten signature purporting to be the signature of the drawer.

But should this nevertheless be viewed as an electronic check in that it is derived from a paper check? Arguably the below definition does not capture this scenario because the sender (the RDC customer) did not itself derive the image from the paper check. It is also likely that the agreement with the receiving bank is written in a manner that requires the depositor to have the physical check or places obligations on the depositor with respect to the physical check that cannot be satisfied without possession.

(ggg) Electronic check and electronic returned check mean an electronic image of, and electronic information derived from, a paper check or paper returned check, respectively,that—

(1) Is sent to a receiving bank pursuant to an agreement between the sender and the receiving bank; and

(2) Conforms with ANS X9.100-187, unless the Board by rule or order determines that a different standard applies or the parties otherwise agree.

(hhh) Electronically-created item means an electronic image that has all the attributes of an electronic check or electronic returned check but was created electronically and not derived from a paper check.

The Study Committee should recommend addressing this issue and consider revising the definition of delivery to capture this scenario and revise 3-105 to eliminate the defense of nonissuance under this scenario, or define an "electronically created item" to cover this scenario and remove it from the scope of Article 3.

Transfer and Presentment Warranties: Early discussions among members of the Payments System Subgroup suggested that the provisions in Regulation CC were sufficient to address "electronic checks" and that changes to the UCC should focus on gaps. Since the May meeting it has been suggested that there may be another gap between Regulation CC and the UCC with respect to the transfer and presentment warranties in UCC Article 3 to the extent UCC Article 3 contemplates transfers or presentments by nonbank entities. After additional discussion it appears that the combination of the Regulation CC warranty and contract is sufficient. No additional action is being recommended at this time.