MEMORANDUM

To: Committee on the Uniform Commercial Code and Emerging Technologies

From: Stephen L. Sepinuck, Associate Reporter

Re: Payments Issues

Date: February 20, 2021

This Memorandum accompanies draft amendments to UCC Articles 3, 4, and 4A dealing with payments issues. The draft amendments are based largely on discussions by the Payments Subcommittee.

The amendments are presented in numerical order of the sections but the subjects they address can be grouped as follows (note, some provisions appear in more than one group because the proposed amendments deal with multiple subjects):

1. Remote Deposit Capture – §§ 3-105, 3-309, 3-604 & 4-209

New technologies have facilitated payment through a process by which a drawer writes and signs a check, takes a photograph of the check, sends the photograph to the drawee for processing electronically, and then destroys the original check. It is unclear under existing law if such check is "issued" within the meaning of § 3-105, and hence a defense of non-issuance is available. The proposed amendments would add language providing that a check can be issued by "electronic transmission," with the result that there would be no defense based on non-issuance. Consideration was given to changing the definition of "delivery" in § 1-201(b)(15),[1] but because that term has relevance to documents of title and chattel paper, it seems advisable to deal with this issue inside Article 3.

When a check is deposited remotely, the check is often purposefully destroyed. If the check image was never received by the depositary bank, and hence no credit was posted to the depositor's account, it is unclear under existing law whether the depositor can pursue a claim under § 3-309, dealing with lost instruments, or whether the intentional destruction of the original check results in a discharge under § 3-604. The proposed amendments would address this by indicating that purposeful destruction of a check in connection with a truncation process, even if by the payee, does not prevent the payee from enforcing the destroyed check if the payment obligation has not been discharged.

Another issue relating to truncation and electronic presentment can arise if a payee remotely deposits a check through electronic means and then negotiates the original paper check to a holder in due course. In such a situation, if the original check is presented to the depositary bank after it has already paid on the electronic presentment, and the depositary bank therefore dishonors the check, the holder in due course will apparently not be able to pursue a claim based

[1] Note, the cross-references in Article 3 to Article 1 are outdated because they refer to the pre-revision version of Article 1. The Committee might wish to consider revising them as part of this process.

on Regulation CC's remote deposit capture warranty because that warranty is not made to a holder of the original check. However, the holder in due course might be able to bring a claim on the instrument against the drawer. It remains unclear whether the drawer would have a defense to payment or a claim against the truncating bank, even though the drawer had no role in the truncation or in the decision to truncate. The proposed amendments to § 4-209(b) would address this situation by creating a warranty that runs to the payor bank and the drawer that the original check will not also be presented for payment.

2. Statement of Account – § 4-406

Section 4-406 deals with a customer's duty to discover and report unauthorized signatures or alterations based on information in a statement of account. The proposed changes to the official text and comments would accomplish two things. First, they would increase the information that the bank must provide in a statement of account to trigger the customer's duty to report. The new information consists of the name of the payee and the date of the item, information which, due imaging technology, banks already regularly provide. Second, they would explain that simply allowing a customer to access the customer's account electronically is not a statement of account.

3. The Scope of Article 4A – Unconditional Promise to Pay – § 4A-104

Article 4A applies to "funds transfers," a term defined to mean a series of transactions that begin with a "payment order." *See* § 4A-102. Pursuant to § 4A-104(a), an instruction qualifies as a "payment order" only if the instruction does not state a condition to payment (other than a time of payment). Proposed amendments to the comments are designed to address whether and how the use of a so-called "smart contract" creates a condition to payment, so as to prevent application of Article 4A to a transaction. The amendments would indicate that a condition in the smart contract itself is not what matters; instead the issue is whether there is a condition in the payment order when that order is received by the receiving bank.

4. Revise Article 4A to Remove the References to a "Writing" – §§ 4A-202, 4A-203, 4A-207, 4A-207 & 4A-305

Each existing reference to a "written agreement" or a similar term has been replaced with a reference to an agreement "evidenced by a record." Each reference to "signed a writing" has been replaced with "authenticated a record."

Three other sections – §§ 4A-103, 4A 210 and 4A 211 – use the phrase "orally, electronically, or in writing" to describe what qualifies as a payment order, a notice of rejection, or a communication of cancellation or amendment. No change to that phrase is proposed because the word "electronically" appears to make a change unnecessary.

5. Security Procedures – §§ 4A-201, 4A-202, 4A-203, 4A-204 & 4A-206

Sections 4A-201 through 4A-204 contain rules on security procedures that can insulate a party from liability in connection with a funds transfer. The proposed amendments are intended to provide additional guidance what new and emerging technologies qualify as a security procedure for the purposes of these provisions, how liability for losses is to be allocated, when a bank acts in "good faith" when accepting a payment order, and when a security procedure is "commercially reasonable." More specifically:

• Section 4A-201 defines the term "security procedure" and provides that a security procedure "may require use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices." Even though that language does not purport to be an exhaustive list, the proposed amendments would add references to "symbols, sounds or biometrics" to make it clear that a requirement of such things can be a security procedure. The amendments would also make it clear that a security procedure can include obligations on the receiving bank and its customer, and that the reasonableness of a security procedure is to be determined at the time a payment order is processed, not at the time the receiving bank and customer agree to the security procedure. The current text states that a signature comparison is not by itself a security procedure. Due to the advent of spoofing and other technologies, the amendments would add that reliance on a known email, IP address or phone number is also not, by itself, a security procedure.

• Section 4A-202 shields from liability a receiving bank that, in good faith, accepts an unauthorized payment order after complying with an agreed-upon, commercially reasonable security procedure. The comments to § 4A-203 explain that the receiving bank has the burden of making a commercially reasonable security procedure available, whereas the customer has the burden of supervising its employees and to assure compliance with the security procedure. Proposed amendments would provide guidance on three issues.

(i) If a third party, whose services are made party of an agreed-upon security procedure, fails to perform its obligations, the proposed amendments would indicate allocation of the loss depends primarily on whether the receiving bank complied with its own obligations under the security procedure. If not, the bank cannot treat the payment order as authorized by the customer.

(ii) If the bank can prove that it did comply with its obligations under the security procedure, the current text of § 4A-203(a) provides that the loss falls on the customer unless the customer can prove that the payment order was not caused by a person entrusted with responsibility for payment orders or someone who obtained access to the customer's facilities. The proposed amendments would add a requirement that the customer also prove that, if the customer failed to comply with its obligations under the security procedure, that failure was not a material cause of the unauthorized payment order. In connection with this, the proposed amendments would amend the text of and comment to § 4A-206, to state that, if a security procedure requires transmission of a payment through a third party, the third party is not thereby an agent of the customer.

(iii) The proposed amendments would state that receiving bank's duty of good faith in processing payment orders does not impose a 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 significantly departs from the customer's prior practices. The draft contains alternative language on this point.

The proposed amendments do not provide additional guidance on whether or how new data-rich payment order formats, heightened supervisory expectations concerning money laundering and fraud, or advances in technology that facilitate near-instantaneous fraud detection affect loss allocation for unauthorized payment orders. Instead, such issues are relegated to the existing standards in Article 4A and to future banking regulations.