REIMAGINING PAYMENT SYSTEMS: ALLOCATION OF RISK FOR UNAUTHORIZED PAYMENT INCEPTION

LINDA J. RUSCH*

INTRODUCTION

Imagine a legal system where the allocation of the risk of an unauthorized debit to a bank account was governed by a simple set of clear rules that did not create different results depending upon the method for initiating the debit. Imagine that the legal rules operated to place incentives on the account owner to safeguard information concerning debiting the account and incentives on the bank holding the account to offer security procedures to assist the account owner in protecting the account from unauthorized access. This is certainly not the world we live in today. Instead, we live in a world where the risk-allocation rules for unauthorized debits to an account operate differently depending upon the mechanism used to access the account. Those risk-allocation rules do not create realistic incentives on either the account owner or the bank holding the account to safeguard against unauthorized debits in a reasonable manner.

The thesis of this article is that it is time to imagine a different way to approach payment systems risk-allocation rules. Instead of being trapped in the past by the way in which different payment systems evolved, it is time to focus on the policies that should be fostered in the payment systems and craft legal rules to advance those policies. Crafting the legal rules should take into account operational realities so as to reduce costs and increase certainty regarding risk allocation. This article will consider one set of policies that may be useful to consider regarding risk allocation for unauthorized debits to a deposit account, that is, fraudulent payment inceptions.

To begin to understand the current payment systems in play, it is necessary to start with a larger picture in order to place the individual pieces in place. First, what is a payment system? At its most basic level, it is a system that is used to transfer value from one person to another in order to pay for goods, services, real estate, or other desired items.[1]

* Frederick N. and Barbara T. Curley Professor of Commercial Law, Gonzaga University School of Law. Thank you to Stephanie Heller for her thoughtful questions and her insight that she shared with me in preparation of this article.

1. *See* BD. OF GOVERNORS OF THE FEDERAL RESERVE SYS., FEDERAL RESERVE POLICY ON PAYMENTS SYSTEM RISK 5–6 (2007) [hereinafter FEDERAL RESERVE POLICY ON PAYMENTS SYSTEM RISK], *available*

The value transferred is generally denominated in standard units as measured by some type of currency, such as dollars or euros.[2] A functioning payment system is a necessary component of economic development. To facilitate the exchange and creation of wealth, payment systems have to be systems of value transfer that function reliably at a reasonable level of cost.[3]

Perhaps the most elementary payment system is physical transfer of currency. To pay for desired commodities or services, a purchaser uses a token, such as a dollar bill, that is deemed to have value by a government[4] and the marketplace.[5] Typically, using currency in this fashion requires physical transfer of the token to another person. In a world where many transactions are not face-to-face and the amounts being transferred are large, physical transfer of large numbers of tokens is not feasible. Thus the modern commercial world has developed alternative mechanisms for making payments.

Payment mechanisms currently in use depend on a system of banking. A person will deposit currency or currency equivalents with a bank and the bank will acknowledge through private agreement with the depositor that the bank owes an obligation to pay demands against that deposit up to the available amount of credit, thus creating a "deposit account." Although that term brings up a mental image of a stash of currency in a vault somewhere at the bank with the depositor's name on it, a deposit account is really just an unsecured debt that the bank owes the depositor.[6]

Demands on the credits the bank owes the depositor come in two basic forms. The depositor may order the bank to transfer credits to

at http://www.federalreserve.gov/paymentsystems/psr/policy07.pdf; FRED H. MILLER & ALVIN C. HARRELL, THE LAW OF MODERN PAYMENT SYSTEMS ¶ 1.01 (2003).

2. *See, e.g.*, U.C.C. §§ 3-104(a) (2005) (negotiable instrument must state a "fixed amount of money"), 4-104(a)(9) (item is a promise or order "to pay money"), 4A-103(a)(1) (payment order must state a "fixed or determinable amount of money"), 1-201(b)(24) (definition of money).

3. *See* Policy Statement—The Federal Reserve in the Payments System, 55 Fed. Reg. 11,648, at 11,649 (Mar. 29, 1990); COMM. ON PAYMENT AND SETTLEMENT SYS., BANK FOR INT'L SETTLEMENTS (BIS), CORE PRINCIPLES FOR SYSTEMICALLY IMPORTANT PAYMENT SYSTEMS § 1.1 (2001) [hereinafter BIS], *available at* http://www.bis.org/publ/cpss43.pdf.

4. Currency and coinage issued by the United States is deemed to be legal tender and is required to be accepted in payment of debts, public and private. 31 U.S.C. § 5103 (2000). *See* Task Force on Stored Value Cards, *A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated With Stored-Value Cards and Electronic Money*, 52 BUS. LAW. 653, 666 (1997).

5. *See generally* SAM Y. CROSS, FED. RESERVE BANK OF N.Y., ALL ABOUT . . . THE FOREIGN EXCHANGE MARKET IN THE UNITED STATES (1998), *available at* http://www.newyorkfed.org/education/addpub/usfxm/.

6. *See, e.g.*, Dean Witter Reynolds, Inc. v. Variable Annuity Life Ins. Co., 373 F.3d 1100, 1107–08 (10th Cir. 2004).

another—a credit transfer (also known as a push transaction). The depositor makes the order that in essence pushes credits from the bank that is "holding" the deposit toward a designated payee. The second method is that a payee, not the depositor, orders the bank that is "holding" the deposit to transfer those credits to the payee—a debit transfer (also known as a pull transaction). The payee "pulls" the credits from the depositor's bank to the payee.[7]

Mechanisms for making these push or pull transactions by giving orders to the bank holding the depositor's credits are as ancient as a draft (which is called a "check" when drawn on a bank)[8] and as modern as an electronic transfer of information from the depositor's bank to the payee's bank over secure computer networks.[9] A check is a debit (pull) transfer; in other words, it is the depositor's (drawer's) order to the drawee bank to pay the designated payee that the payee (or a bank acting on behalf of the payee) presents to the drawee bank.[10]

Now consider a more modern payment mechanism for ordering payment from a bank account: electronic bill-paying interfaces. These interfaces can be either credit or debit transactions. A credit transaction is illustrated by the depositor accessing its bank's website and using a computerized instruction interface to order that bank to make payment to the designated payee using credits from the depositor's bank account.[11] A debit transaction is illustrated by the depositor visiting a payee's website and, through a computerized instruction to the payee, authorizing the payee to pull credits from the depositor's bank account to the payee's bank account.[12] The depositor or payee does not have to initiate the credit or debit transaction each time a payment

7. *See* U.C.C. art. 4A prefatory note; James Steven Rogers, *The Basic Principle of Loss Allocation for Unauthorized Checks*, 39 WAKE FOREST L. REV. 453, 456–57 (2004).

8. U.C.C. § 3-104(f).

9. This is the type of system described in the prefatory note to U.C.C. Article 4A.

10. U.C.C. §§ 3-103(a)(8) (definition of order), 3-103(a)(5) (definition of drawer), 3-104(e) (draft as an order to pay), 3-501 (presentment), 3-502(b) (dishonor), 4-104(a)(8) (definition of drawee), 4-105(3) (definition of payor bank), 4-201 (collecting bank as agent for owner of item). Even with the depositor's instruction (the check), the drawee bank is not obligated to the payee to transfer any value to the payee. *Id.* § 3-408. The drawee bank's refusal to pay a payee as ordered by the drawer may give the drawer a cause of action against the drawee bank for wrongful dishonor based upon breach of the deposit agreement between the drawee and drawer. *Id.* § 4-402. In U.C.C. Article 4 terminology, the drawee bank is the payor bank, *id.* § 4-105(3), and the drawer is the customer of the payor bank, *id.* § 4-104(a)(5).

11. *See also* Nancy Feig, *Bank of America Achieves Highest Adoption of Online Bill Pay Among Leading Banks*, FINANCETECH, Mar. 6, 2007, http://www.financetech.com/showArticle.jhtml?article ID=197800476 (discussing the prevalence of online bill payment services).

12. *See* Ronald J. Mann, *Regulating Internet Payment Intermediaries*, 82 TEX. L. REV. 681, 687–88 (2004).

is due. A depositor may sign a written authorization allowing a payee to pull funds from the depositor's account automatically at certain time intervals. A depositor may also sign a written authorization allowing its bank to push payments to payees at designated intervals. Reoccurring payments, such as mortgages or insurance premiums, may be handled in this more automated way.[13] A depositor may also use an access mechanism such as a debit card to instruct its bank to transfer credits to a payee at the point of sale. This is common in retail sales of merchandise.[14]

The legal rules that govern the various methods of instructing the depositor's bank to move credits to payees have evolved over time and differ significantly depending in large part on the method of giving the instruction to the bank holding the account. Thus the rules governing checks are significantly different than the rules governing electronic credit or debit transactions. Uniform Commercial Code (U.C.C.) Articles 3 and 4 will govern checks drawn on the payor (depositor's) bank, but not the payor's instructions made in some other manner to move value from its bank to a payee.[15] Many transactions in which the payor's instruction to its bank is made through some mechanism other than a check are governed by U.C.C. Article 4A, or funds-transfer system rules, such as those promulgated for the Automated Clearing House network (ACH).[16] Some debit transactions (instructions given by a payee through a mechanism other than a check) are not governed by the U.C.C. at all. Rather, many debit transactions are governed by common

13. *See* 12 C.F.R. § 205.10(b) (2007).

14. *See, e.g.*, PAYMENT SYS. POLICY ADVISORY COMM., FED. RESERVE BD., A SUMMARY OF THE ATLANTA FORUM ON TRANSFORMING U.S. RETAIL PAYMENTS (2006), *available at* http://www.federalreserve.gov/paymentsystems/transformretail/transformretail.pdf. For a comparison of echecks and debit cards, see eCheck, Comparison with Other Payment Instruments: Debit Cards, http://www.echeck.org/overview/comparison/debitcard.html (last visited Feb. 20, 2008).

15. *See* U.C.C. §§ 3-102(a) (Article 3 applies to negotiable instruments), 3-104 (check as a negotiable instrument), 4-102 (Article 4 applies to items), 4-104(a)(9) (definition of item includes instrument); Stephanie Heller, *An Endangered Species: The Increasing Irrelevance of Article 4 of the UCC in an Electronics-Based Payments System*, 40 LOY. L.A. L. REV. 513, 514–16 (2006) (explaining the limitation of Articles 3 and 4 to "writings"). Some uncertainty currently exists in determining application of the rules in some circumstances when a check is involved in starting the payment instruction but at some point during that process the paper check is no longer being used, rather the instruction is being carried out based upon information derived from the paper check. *See infra* text accompanying notes 103–10.

16. U.C.C. §§ 4A-102 (application to funds transfers), 4A-104 (definition of funds transfers), 4A-104 cmt. 4 (application to credit transfers only); NAT'L AUTOMATED CLEARING HOUSE ASS'N, 2007 ACH RULES: A COMPLETE GUIDE TO RULES AND REGULATIONS GOVERNING THE ACH NETWORK (2007) [hereinafter 2007 ACH RULES]. *See infra* notes 163–82 and accompanying text on the ACH rules that are promulgated by NACHA. More information about NACHA may be obtained at http://www.nacha.org/About/default.htm.

law contract, property, and tort principles, as there is not a body of codified law that uniformly applies.[17] If a debit transaction is made through a network such as ACH, funds-transfer system rules will apply.[18]

The identity of the payor will also determine what legal rules apply in the event of an electronic credit or debit transaction. If the payor is a consumer and the deposit account is held primarily for family, personal, or household purposes of the consumer, a different set of legal rules will apply than if the deposit account is not held for such purposes.[19] The federal Electronic Funds Transfer Act (EFTA)[20] and Regulation E[21] will govern some, but not all, aspects of the relationship between the consumer and the depositary bank. Those federal rules are primarily focused on some principles of consumer protection, as opposed to a wholesale regulation of the funds transfer from start to finish.[22]

In thinking about deposit accounts, one can easily imagine the various types of risk involved in this arrangement for making payments, no matter what mechanism is used to initiate the payment. First, there is always a credit risk. Credit risk refers to the risk that the depositor may not have available value in the deposit account to cover the instruction to push or pull value from the account.[23] The payee takes that credit risk if it parts with its value before the payment transaction is complete. The depositary bank takes that risk if it honors the payment push or pull even if the value of credits allocated to the deposit account is insufficient. Second, there may be some risk of intermediary failure in any payment transaction utilizing the banking system. This risk occurs when the depositary bank, intermediary bank, or non-bank intermediary fails or is unable to complete the payment transaction due to failure of its processing system.[24] Who bears that

17. *See* 3 JAMES J. WHITE & ROBERT S. SUMMERS, UNIFORM COMMERCIAL CODE § 22-2, at 3–4, 11–15 (West Pub. Co., Practitioner Treatise Series, 4th ed. 1995).

18. 2007 ACH RULES, *supra* note 16.

19. 12 C.F.R. §§ 205.3 (scope of Regulation E), 205.2(b) (definition of account), 205.2(e) (definition of consumer) (2007).

20. Pub. L. No. 95-630, Title XX, 92 Stat. 3641, 3728 (1978) (codified as amended at 15 U.S.C. §§ 1693–1693r (2000)).

21. 12 C.F.R. pt. 205.

22. *See* 12 C.F.R. § 205.1(b).

23. *See* FEDERAL RESERVE POLICY ON PAYMENTS SYSTEM RISK, *supra* note 1, at 3. The Federal Reserve distinguishes credit risk (failure of settlement when due and thereafter) from liquidity risk (failure to pay when due). *Id.*

24. *Id.* The Federal Reserve lumps both intermediary failure risk and fraud risk into a larger category it denominates "operational risk," that is, "risk of loss resulting from inadequate or failed

risk in any payment transaction will depend upon the mechanism used to initiate the payment.[25] Another article in this symposium considers the risk of intermediary failure.[26]

A third risk, closely related to intermediary failure, is the risk that mistakes will be made in the payments processing system. Typical types of mistakes are (i) mistakes in identifying the correct depositary account, the correct payee account, or the correct payee, or (ii) errors in the amount of the value transfer or the timing of the value transfer.[27] Again, other articles in this symposium consider those types of risks.[28]

A fourth risk in any payment system is the risk that the costs of operating the system using any particular mechanism make the system unattractive as a method for making payments.[29] Costs of operating a system include not only direct costs of equipment, personnel, and infrastructure for processing, but also many types of indirect costs. These indirect costs include the costs of obtaining cooperation between the players in the system so that the system functions, costs of reallocating the losses that inevitably will happen in any payment system, and costs of educating the users regarding the system. The direct and indirect costs of any payment system are ultimately born by all of the players in the system.[30] How these costs are spread among the players is often not transparent or obvious.

Finally, there is a fraud risk in any payment system. One type of fraud risk exists when the purported payor does not actually have the right to push value from the account in a particular transaction or where the payee does not actually have the right to pull value from the account.[31] Typically, the wrongdoer that fraudulently initiates the or-

internal processes, people, and systems, or from external events. This type of risk includes various physical and information security risks." *Id.*

25. *See* U.C.C. art. 4A prefatory note (2005) (discussion of insolvency losses).

26. *See* James Stevens Rogers, *Unification of Payments Law and the Problem of Insolvency Risk in Payment Systems*, 83 CHI.-KENT L. REV. 689 (2008).

27. *See, e.g.*, U.C.C. §§ 4-209 (encoding errors), 4A-205 (late or erroneous execution of payment order), 4A-207 (misdescription of beneficiary), 4A-208 (misdescription of bank); Richard F. Dole, Jr., *Receiving Bank Liability for Errors in Wholesale Wire Transfers*, 69 TUL. L. REV. 877 (1995).

28. *See* Sarah Jane Hughes, *Duty Issues in the Ever-Changing World of Payments Processing: Is it Time for New Rules?*, 83 CHI.-KENT L. REV. 721 (2008); Anita Ramasastry, *Confusion and Convergence in Consumer Payments: Is Coherence in Error Resolution Appropriate?*, 83 CHI.-KENT L. REV. 813 (2008).

29. *See* BIS, *supra* note 3, § 2.4.

30. *See id.* §§ 3.8.1–.8.6, 7.8.6–.8.13.

31. *See generally* A. Brooke Overby, *Check Fraud in the Courts After the Revisions to U.C.C. Articles 3 and 4*, 57 ALA. L. REV. 351 (2005).

der to debit the payor's account cannot be found or does not have sufficient value available to make the purported payor whole. If recovery is unavailable for some reason against the wrongdoer, then one of the parties to the payment transaction will bear that risk, even if that party acted innocently and with all due care. The risk of this type of fraud could rest on the payee, the payee's bank, the purported payor, or the payor bank. Where that risk ultimately resides depends upon a complicated set of payment rules that further depend on the status of the purported payor, the mechanism used to initiate payment, the method used to process the payment, and the means by which the fraud was perpetrated.

It is that risk of fraud in the inception of the payment process that is the subject of this article. Part I of this article will set forth the current risk-allocation rules for unauthorized debits from a bank account, regardless of whether the transaction is a push or pull transfer. Part II will explore possible principles for guiding risk allocation and factors that may influence the choice of one or more of those principles as the basis for a more simplified set of rules for risk allocation. In doing so, possible draft rules will be proposed and discussed. Part II will also evaluate the attractiveness of the possible draft rules in any payments reform effort in light of operational realities. The purpose of this evaluation is to demonstrate that payments rules may be crafted from a policy perspective in a functional manner and need not be based on the manner in which the instruction is made to the payor bank.

I. ALLOCATION OF THE RISK OF UNAUTHORIZED PAYMENT INCEPTION UNDER CURRENT LAW

This section briefly explains how the current legal rules allocate the risk of unauthorized debits from a deposit account by first considering the rules regarding checks. After a review of the check mechanism, this section will explore push and pull payment orders other than checks.

A. Checks

U.C.C. Articles 3 and 4 provide the main source of legal rules for allocating the risk of an unauthorized debit from a deposit account using a check. This discussion will assume the traditional paradigm of the check as a paper instrument that the purported payor issues to the payee and the payee presents to the payor bank for payment. After that

discussion, the legal rules that may apply if the check is not processed all the way through to the payor bank in its original paper format will be addressed.

To flesh out a basic understanding of the allocation of risk for unauthorized checks, a simple scenario is discussed below. In the first example, there is no unauthorized issuance of the check. In the second example, there is an unauthorized issuance of the check. In that discussion, what counts as "unauthorized" is also considered.

1. Example 1: Authorized Issuance

Davis (the payor) has a deposit account at First Bank (the payor bank). Davis signed a check drawn on First Bank and issued to Phil (the payee). Phil deposits the check to his account at National Bank (the payee's bank). National Bank presents the check to First Bank for payment. First Bank pays the value for the check to National Bank, and National Bank gives Phil a credit for that amount to Phil's bank account. First Bank deducts the amount of the check from Davis's deposit account at First Bank.

In U.C.C. Article 3 terminology, the person that issues a check to a payee is the drawer (the payor).[32] By signing the check, Davis, the drawer, is ordering the drawee (the payor bank, First Bank) to make payment of the amount of the check to the payee designated on the check, in this case, Phil.[33] National Bank (the payee's bank) is acting as Phil's agent in collecting the amount of the check from First Bank.[34]

Davis's signature on the check also creates an obligation of Davis to pay the amount of the check to Phil in the event First Bank dishonors the check.[35] Davis's issuance of the check to Phil, without more, does not create any enforceable right of Phil to compel First Bank to honor the check or to pay value to Phil.[36] If First Bank dishonors the check when National Bank presents the check, then National Bank will charge back the amount of the dishonored check against Phil's account with National Bank.[37] Phil will then have to rely on his right to enforce

32. U.C.C. § 3-103(a)(5).

33. *Id.* §§ 3-103(a)(8) (definition of order), 3-109 (payable to order or bearer).

34. *Id.* § 4-201.

35. *Id.* § 3-414. This liability is often referred to as contract liability on the draft. *See* Barry L. Zaretsky, *Contract Liability of Parties to Negotiable Instruments*, 42 ALA. L. REV. 627 (1991).

36. U.C.C. § 3-408. This statement is true as long as the drawee has not "accepted" the check. Acceptance of the check is the drawee's signed engagement on the check to pay it. A certified check is an example of an "accepted" check. *Id.* § 3-409. If the drawee has signed the check, thus creating an "accepted" check, the drawee will then have an obligation to pay the check. *Id.* § 3-413.

37. *Id.* § 4-214.

Davis's liability as a drawer on the check through a lawsuit in the event Davis does not pay voluntarily.[38] In that lawsuit, Davis may have defenses to payment that he could assert against Phil.[39]

If First Bank honors the check, First Bank will pay the amount of the check to National Bank. This payment often takes place by crediting an account of National Bank with First Bank or debiting an account of First Bank at National Bank.[40] First Bank will deduct the amount of the value of the check from the deposit account of Davis.[41] First Bank has a right to deduct the value of the check from the deposit account of Davis if the check is "properly payable" from the account. A check is properly payable if "it is authorized by the customer and is in accordance with any agreement between the customer and bank."[42] The drawer of the check (the payor) is the "customer" of the drawee (the payor bank) on which the check is drawn.[43] Generally, if the drawer has signed the check or authorized the drawer's signature on the check and the payee receives the value from the check, the check is properly payable from the drawer's account with the drawee bank.[44]

Now consider how the rules work when the person who signs the check as the drawer is not authorized to sign the check.

38. *Id.* § 3-414.

39. A drawer obligated on the check will be presumptively liable unless it raises a defense to payment when it is sued based upon the drawer's liability under U.C.C. section 3-414. *Id.* § 3-308. The type of defenses that may be asserted are provided for in U.C.C. section 3-305. Some typical defenses may be that the value given for issuance of the check was not actually provided, the drawer did not sign or authorize the signing of the check, the check has already been paid, or the check has been altered. *See id.* § 3-305 cmts. 1–2. Whether those defenses will be successful depends in part on whether the person seeking to enforce the drawer's liability is a holder in due course that has taken free of that defense. *Id.* §§ 3-302 (requirements of a holder in due course), 3-305(b) (holder in due course not subject to certain types of defenses).

40. *Id.* §§ 4-301 (payor bank provisional settlement), 4-215 (payor bank final payment), 4-213 (types of settlements).

41. *Id.* § 4-401.

42. *Id.* § 4-401(a).

43. *Id.* § 4-104(a)(5).

44. *See* 7 LARY LAWRENCE, LAWRENCE'S ANDERSON ON THE UNIFORM COMMERCIAL CODE § 4-401:5 (rev. 3d ed. 2000). Typically, the bank-customer agreement will provide that the drawee bank is authorized to charge the drawer's deposit account whenever the drawer signed the check or authorized the drawer's signature on the check. *But see* Paul S. Turner, *Contracting Out of the UCC: Variation by Agreement Under Articles 3, 4, and 4A*, 40 LOY. L.A. L. REV. 443, 448–50 (2006) (describing bank-customer agreements that shift the responsibility for unauthorized checks to the drawer); *see also* Gregory E. Maggs, *A Complaint About Payment Law Under the U.C.C.: What You See Is Often Not What You Get*, 68 OHIO ST. L.J. 201, 203–06 (2007).

2. Example 2: Unauthorized Issuance

Davis has a deposit account at First Bank. Francis (the wrongdoer) signed a check drawn on Davis's account at First Bank and gave that check to Phil. Davis has not authorized Francis to draw any checks on his account at First Bank. Francis obtained a check blank from Davis by stealing Davis's checkbook. Phil deposits the check to his account at National Bank. National Bank presents the check to First Bank for payment. First Bank pays the amount of the check to National Bank and National Bank gives Phil a credit for that amount to Phil's bank account. First Bank deducts the amount of the check from Davis's deposit account at First Bank.

Francis's signature on the check creates an obligation of Francis, not Davis, to pay the amount of the check to Phil in the event First Bank dishonors the check.[45] If First Bank dishonors the check when National Bank presents the check, then National Bank will charge back the amount of the dishonored check as against Phil's account with National Bank.[46] Phil will then have to rely on his right to enforce Francis's liability as a drawer on the check through a lawsuit in the event Francis does not pay voluntarily. In that lawsuit, Francis may have defenses to payment that could be asserted against Phil.[47] If Phil tries to sue Davis on the drawer's contract obligation on the check, which may happen if Francis has signed Davis's name on the check, Davis has a viable defense to payment because it is not his authorized signature.[48] This defense can be asserted against Phil (or National Bank) even if one or the other qualifies as a holder in due course of the check.[49]

If First Bank honors the check with the unauthorized drawer's signature, First Bank has no right to charge Davis's deposit account with First Bank as the check is not "properly payable" from the ac-

45. U.C.C. §§ 3-403 (liability of unauthorized signor), 3-414 (drawer's liability).

46. *Id.* § 4-214.

47. *See supra* note 39.

48. U.C.C. §§ 3-401, 3-403. To place the validity of the drawer's signature in issue, Davis must specifically deny that it was his signature in the pleadings when action is brought to enforce the drawer's liability. In that circumstance, the person seeking to enforce the drawer's liability on the check would have to prove that the signature was valid or that the drawer should be held liable on the check. *Id.* § 3-308(a).

49. A holder in due course is entitled to enforce the "drawer's" obligation on the instrument free from most defenses to payment. *Id.* §§ 3-414, 3-305. Whether a signature is authorized determines who is the "drawer" of the check. That is why Article 3 provides that a person is not liable on the instrument unless that person signed the instrument or is responsible for the signature, *id.* § 3-401, and that the signature of an unauthorized signor operates to bind the unauthorized signor, not the person whose name was signed. *Id.* § 3-403.

count.[50] The check did not authorize payment to Phil from Davis's account because Francis was not authorized to issue the check drawn on Davis's account. Thus Davis will be able to successfully require that First Bank recredit his account for the value previously deducted from the account. First Bank will then seek to recover the value for the check from National Bank or Phil.

Unless one of a variety of exceptions applies, First Bank will not be able to recover the value of the check from either National Bank or Phil once First Bank has made "final payment" on the check. First Bank has made final payment on the check if it makes a provisional settlement for the check with National Bank by midnight of the banking day of receipt and fails to timely return the check by its midnight deadline.[51] First Bank generally will make a provisional settlement with National Bank for the amount of the check when National Bank presents the check to First Bank. The midnight deadline is midnight of the banking day following the banking day that First Bank received the check.[52] Because the authorized drawer (Davis) may not discover for some time that an unauthorized check was drawn on the account, and thus may not raise the argument that the check was not properly payable until well beyond the drawee bank's (First Bank's) midnight deadline, First Bank will bear the loss, as it will not be able to rightfully return the check to National Bank or Phil before expiration of its midnight deadline.[53]

3. Authorized by the Drawer

When is a check authorized by the drawer? First and foremost, a check is authorized by the drawer if the drawer signed the check that orders payment to the payee, and the payee (or the payee's designee)

50. *Id.* § 4-401 cmt. 1.

51. *Id.* §§ 4-301 (ability to revoke a provisional settlement), 4-215 (when final payment has been made). Return of a check happens when the drawee bank "sends" the check. Sending means to deliver the check for transmission with the costs of transmission provided for. *Id.* § 1-201(b)(36). Thus, to comply with the midnight deadline, the drawee bank must get the check to the means of transmission by that deadline, but is not required to ensure that the bank to which the check is sent actually receives the check.

52. *Id.* § 4-104(a)(10). In some circumstances, the midnight deadline may be extended if the drawee bank has used a very expeditious means of returning the check so that it would arrive at the bank to which it was returned in the same time frame it would have arrived if the drawee bank had met the midnight deadline. 12 C.F.R. § 229.30(c) (2007).

53. *See infra* notes 74–88 and accompanying text on the typical inability of the payor bank to pass the loss from a check with a forged drawer's signature back to the payee's bank.

is the one receiving the value from the drawee.[54] Second, the check is authorized by the drawer if the drawer authorized another person to draw the check on the drawer's deposit account payable to the payee and the payee (or the payee's designee) receives the value. The drawer's authorization is created according to normal rules of agency law, including apparent authority.[55] Third, the check is authorized by the drawer if the drawer and the drawee bank agree by contract to alter the usual rules of authorization stated above.[56] For example, in a positive pay agreement the drawee and the drawer agree that the drawee will honor all checks identified on a list provided by the drawer, regardless of whether the check is in fact signed or authorized by the drawer under agency principles. The identification of the checks on the list is often by check number and amount.[57] The following discussion assumes that the purported drawer's signature on the check is in fact unauthorized.

4. Exceptions to the Allocation of Risk of Unauthorized Drawer's Signature to the Drawee Bank

As referred to above, there are numerous exceptions to the general rule that allocates the risk of an unauthorized drawer's signature to the drawee bank that has made final payment on the check. In some circumstances, the risk will be allocated to the purported drawer; in

54. U.C.C. §§ 3-401, 4-401 cmt. 1. The payee's designee is the person to whom the payee has delivered the check for collection (such as a depositary bank) or the person whom the payee has designated should receive payment, such as a transferee. If the payee's necessary indorsement is forged, the payee has not designated anyone to receive payment on the check. A payee's indorsement is "necessary" when the check is payable to the named payee and in order to further negotiate the check, the payee must indorse the instrument. *Id.* § 3-205. Thus, the first comment to U.C.C. section 4-401 states that items that contain forged indorsements are not properly payable. When the payee's necessary indorsement is forged, the loss is generally passed back to the bank in which the check was deposited based upon breach of a presentment warranty. *Id.* § 3-417(a)(1) (warranty that prior transferor was entitled to enforce). If a check is payable to the named payee, only the named payee is "entitled to enforce" the check until the payee indorses the check or voluntarily transfers the check to another. *Id.* §§ 3-301 (entitled to enforce), 3-203 (transfer of instrument), 1-201(b)(21) (definition of holder). If the payee's necessary indorsement is forged and the check is paid through the bank collection process, the payee will have a cause of action for conversion against the depositary bank or other persons who took the check after the forged indorsement. *Id.* § 3-420.

55. *Id.* § 3-402(a).

56. The extent to which the bank-customer agreement in fact changes the allocation of the risk of an unauthorized signature to the customer may be unclear, such as in the case of a facsimile signature. *See* Lor-Mar/Toto, Inc. v. 1st Constitution Bank, 871 A.2d 110 (N.J. Super. Ct. App. Div. 2005); Turner, *supra* note 44, at 449–52.

57. *See* Subcomm. on Payments, Am. Bar Ass'n, *Deterring Check Fraud: The Model Positive Pay Services Agreement and Commentary*, 54 BUS. LAW. 637, 644–45 (1999).

other circumstances, the risk will be allocated to the payee or the payee's bank.

a. Risk on the Purported Drawer

First, consider how the risk of an unauthorized drawer's signature may be allocated to the purported drawer. As discussed above, the drawee bank may only charge the drawer's account for an item that is properly payable. A check with a forged drawer's signature is not properly payable.[58] If the drawer seeks to obtain a recredit to its account based upon an argument that the check with the forged drawer's signature is not properly payable, the drawee bank may counter with an argument that the purported drawer was negligent and that negligence substantially contributed to the making of the forgery of the drawer's signature on the check, thus precluding the purported drawer from asserting that forgery against the drawee bank.[59] Thus, in Example 2 discussed above, First Bank would try to demonstrate that Davis was negligent and his negligence substantially contributed to Francis forging Davis's signature on the check. If First Bank was successful in that argument, then Davis would argue that First Bank was also negligent in paying the check and that First Bank's negligence substantially contributed to the loss. In that event, the loss is shared between Davis and First Bank based upon the relative degree of negligence of the parties.[60] Unfortunately for Davis, however, he will often be unable to assert that First Bank's negligence consisted of the failure to examine the drawer's signature on the check. Under U.C.C. Articles 3 and 4, a drawee bank is not lacking ordinary care if it pays a check without examination of the signature, as long as the bank follows its prescribed procedures and those procedures "do not vary unreasonably from

58. *See supra* notes 42 & 50 and accompanying text. In any of the situations discussed in the text where the drawee/payor bank is able to allocate the risk of the forged drawer's signature to the drawer, the drawer may want to sue the wrongdoer or those parties that took the check from the wrongdoer. Whether the drawer has a cause of action in this situation is very uncertain. *See* Philip E. Cleary, *Statutory Overkill: Why Section 3-420(a) of the Uniform Commercial Code May Not Really Mean What It Says About the Issuer's Cause of Action for Conversion of a Negotiable Instrument*, 39 UCC L.J. 399 (2007).

59. U.C.C. § 3-406(a). The negligence based preclusion in section 3-406 applies to a forgery of the drawer's signature. A forgery is just one of the ways in which a drawer's signature may be unauthorized. *See id.* §§ 1-201(b)(41), 3-406 cmt. 2.

60. *See id.* § 3-406(b). That subsection provides:

> [I]f the person asserting the preclusion fails to exercise ordinary care in paying or taking the instrument and that failure substantially contributes to loss, the loss is allocated between the person precluded and the person asserting the preclusion according to the extent to which the failure of each to exercise ordinary care contributed to the loss.

general banking usage not disapproved by [Articles 3 or 4]."[61] In Example 2, Davis might be negligent in the circumstances that allowed Francis access to the check blank, and that negligence may be sufficient to preclude Davis from asserting the forgery of his signature on the check against First Bank.

Davis may also be precluded from asserting against First Bank the forgery of his signature on the check if First Bank makes available a statement showing payments made from the deposit account, and Davis fails to examine the statement and notify First Bank of the unauthorized check in a timely manner.[62] This "bank statement rule" has three separate and distinct aspects.

First, if Davis fails to report the unauthorized check within a reasonable time after the statement is made available to him, and First Bank proves it suffered a loss by virtue of Davis's failure to examine and to report the problem promptly to First Bank, Davis is precluded from asserting the unauthorized signature against First Bank in the action to get First Bank to recredit the account pursuant to the properly payable rule.[63] This rule will allocate the risk to Davis generally only if First Bank can demonstrate that the time lag in reporting prevented successful recovery of the amount of the check from the wrongdoer.[64]

Second, if Davis fails to report an initial unauthorized check in a timely manner after a statement is made available and the same wrongdoer obtains payment on a second unauthorized check after Davis had a reasonable time (not to exceed thirty days after the account statement was made available to Davis) to report the first unauthorized check, Davis is precluded from asserting the forgery on the second unauthorized check.[65]

In both of those circumstances, Davis has a slim opportunity to split the loss with First Bank using comparative negligence principles if Davis can prove that First Bank failed to use ordinary care in paying the item and that failure substantially contributed to the loss.[66] This

61. *Id.* § 3-103(a)(9); *see, e.g.*, Union Planters Bank, Nat'l Ass'n v. Rogers, 912 So.2d 116, 123–24 (Miss. 2005); Mark E. Budnitz, *The Consequences of Bulk in Our Banking Diet: Bulk Filing of Checks and the Bank's Duty of Ordinary Care Under the 1990 Revision to the Uniform Commercial Code When it Honors Forged Checks*, 63 TEMP. L. REV. 729, 776–77 (1990).

62. U.C.C. § 4-406(c).

63. *Id.* § 4-406(d)(1).

64. *Id.*; *see* LAWRENCE, *supra* note 44, § 4-406:18.

65. *See* U.C.C. § 4-406(d)(2).

66. *See id.* § 4-406(e).

argument suffers from the same difficulty in showing First Bank failed to use ordinary care, as considered previously. Generally, First Bank's payment of the check using automated means or its failure to examine the signature will not show a lack of ordinary care.[67] In both situations described above, Davis may also attempt to show that First Bank failed to pay the item in good faith in order to preclude First Bank from using either rule to preclude Davis's assertion of the forged drawer's signature.[68] This is not an easy standard for Davis to meet, even though the standard of good faith includes honesty in fact and the exercise of reasonable commercial standards of fair dealing.[69]

Finally, the bank statement rule has a third aspect. Regardless of the lack of care of either the drawee bank or the purported drawer, the purported drawer is precluded from asserting the forged drawer's signature against the drawee bank if the purported drawer does not discover or report the unauthorized signature within one year after the statement of account is made available to the purported drawer.[70] Courts have upheld the drawee bank's shortening of this time period in the bank-customer agreement.[71]

The drawee bank has one more argument to assert against the purported drawer to preclude that person from asserting the drawer's signature was unauthorized when the purported drawer makes the argument that the check was not properly payable. If the purported drawer ratifies an otherwise unauthorized drawer's signature, the purported drawer will be precluded from asserting that the check was not properly payable.[72] Ratification is a "retroactive adoption of the unauthorized signature by the person whose name is signed" and is effective for all purposes except as for allocation of liability as between the unauthorized signor and the purported drawer.[73]

67. *See supra* note 61 and accompanying text.

68. *See* U.C.C. section 4-406(e) which provides in relevant part: "If the customer proves that the bank did not pay the item in good faith, the preclusion under subsection (d) does not apply."

69. *See id.* §§ 3-103(a)(6), 4-104(c), 1-201(b)(20).

70. *Id.* § 4-406(f).

71. *See, e.g.*, Nat'l Title Ins. Corp. Agency v. First Union Nat'l Bank, 559 S.E.2d 668, 672 (Va. 2002) (sixty days); Am. Airlines Employees Fed. Credit Union v. Martin, 29 S.W.3d 86, 97–98 (Tex. 2000) (same); Stowell v. Cloquet Co-op Credit Union, 557 N.W.2d 567, 572 (Minn. 1997) (twenty days from mailing statement); *cf.* Regatos v. N. Fork Bank, 838 N.E.2d 629, 633 (N.Y. 2005) (bank-customer agreement could not shorten the one year time period in U.C.C. section 4A-505).

72. U.C.C. § 3-403(a).

73. *Id.* § 3-403 cmt. 3.

b. Risk Allocated to the Payee or Payee's Bank

First Bank (the drawee bank), if unable to reallocate the loss on the unauthorized check to Davis (the purported drawer) through the mechanisms described above, will seek to transfer the loss "upstream" to the payee's bank or the payee.[74] Once final payment has taken place on the unauthorized check, the drawee bank has a very limited ability to attempt to collect from the entity that presented the check or prior transferors of the check. The drawee bank may assert a right to restitution, a breach of a presentment warranty, or that the payee's bank or the payee was part of a scheme to defraud the drawee bank.

Using the facts from Example 2 described above, First Bank (the drawee bank) has the ability to seek restitution from National Bank (the payee's bank) when First Bank pays the check based upon the unauthorized signature, even if First Bank has not exercised ordinary care.[75] Unfortunately for First Bank, however, National Bank will usually be able to have a complete defense to the restitution argument if National Bank took the check in good faith and for value from Phil, the payee.[76] Typically, National Bank will have acted in good faith in taking the check for deposit from Phil and will have given Phil value in the form of credit to Phil's account.[77] Restitution is thus not often a fruitful loss reallocation mechanism for drawee banks that have paid a check with an unauthorized drawer's signature given this protection of a good faith taker of the check who has given value for the check.[78]

First Bank may attempt to assert breach of a presentment warranty by National Bank and Phil. A person obtaining payment of a check (the presenting bank, National Bank) and each prior transferor (Phil) warrant to the drawee that has paid an item (First Bank) that the warrantor has "no knowledge that the signature of the purported drawer of the draft is unauthorized."[79] Knowledge means "actual knowledge" and does not mean "reason to know" based upon known

74. Under the bank-customer agreement between National Bank (the payee's bank) and Phil (the payee), National Bank will undoubtedly have recourse against Phil if National Bank has to pay the drawee bank, First Bank. *See id.* §§ 4-214, 4-103.

75. *See id.* § 3-418(a).

76. *See id.* § 3-418(c).

77. *See id.* § 3-303 (definition of value).

78. Persons protected from restitution are those that took the check in "good faith and for value" or changed position in good faith reliance on the payment. *Id.* § 3-418(c); *see* 6 WILLIAM D. HAWKLAND & LARY LAWRENCE, UNIFORM COMMERCIAL CODE SERIES: REVISED ARTICLE 3 NEGOTIABLE INSTRUMENTS § 3-418:5 [Rev] (Supp. 2007).

79. U.C.C. § 4-208(a)(3); *cf.* § 3-417(a)(3).

facts and circumstances.[80] In most situations, the payee will not know that the drawer's signature was not authorized and neither will the presenting bank.[81] Thus this presentment warranty is also not usually a promising avenue of recovery for the drawee bank. Even if the payee or presenting bank knew that the drawer's signature was unauthorized, the drawee bank will be unable to recover on the presentment warranty if the drawee bank should have asserted the one-year preclusion against the purported drawer under the bank statement rule as discussed earlier.[82]

Amendments to Regulation CC provide for a new presentment warranty made to a drawee bank that pays a particular type of check that that check is in fact authorized by the drawer.[83] The type of check to which this new warranty applies is a "remotely created check." A remotely created check is a check that "is not created by the [drawee] bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn."[84] While ambiguities abound with this definition, the idea of the section is to allow the loss to be passed to the bank that took the check from the payee for checks drawn on deposit accounts with notations such as "authorized by drawer," when the check was not in fact so authorized.[85] The Regulation CC commentary states that this definition does not apply to checks where the drawer's signature is forged.[86] This Regulation CC warranty is also subject to defeat if the drawee bank has

80. *Id.* § 1-202(b).

81. *See* Overby, *supra* note 31, at 363.

82. U.C.C. § 4-406(f); *see supra* notes 62–71 and accompanying text. Similarly, U.C.C. section 4-208(c) provides that if the drawee bank asserts a claim for breach of a presentment warranty based upon an alteration or an unauthorized indorsement, the drawee bank cannot recover on the presentment warranty if it should have asserted either the negligence preclusion in U.C.C. section 3-406 or the preclusion in U.C.C. section 4-406 (bank statement rule). Interestingly, U.C.C. section 4-208(c) does not preclude the drawee bank from asserting a breach of presentment warranty based upon an unauthorized drawer's signature if the drawer would be precluded from asserting the lack of authorization under either U.C.C. section 3-406 or section 4-406.

83. *See* Collection of Checks and Other Items by Federal Reserve Banks, 70 Fed. Reg. 71,218 (Nov. 28, 2005) (effective July 1, 2006) (codified at 12 C.F.R. § 229.34(d) (2007)). This change was made after the National Conference of Commissioners on Uniform State Laws and the American Law Institute promulgated amendments to Articles 3 and 4 providing for a new presentment warranty that the drawer's signature was actually authorized on a remotely created consumer check that the drawee bank paid when presented. U.C.C. §§ 3-417(a)(4), 4-208(a)(ii)(4). A remotely created consumer item is defined as "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." *Id.* § 3-103(a)(16). A consumer account is an "account established by an individual primarily for personal, family, or household purposes." *Id.* § 3-103(a)(2).

84. 12 C.F.R. § 229.2(fff) (2007).

85. 12 C.F.R. pt. 229, app. E, § II(FFF).

86. *Id.*

failed to assert the bank statement rule preclusions against the purported drawer.[87] Only banks make the new Regulation CC warranty. Thus, if the presenting bank or other transferor bank has breached this warranty, the bank-customer agreement between the payee and its bank (which will either be a presenting bank or a transferor bank) will be the mechanism to pass the loss to the payee based upon the unauthorized drawer's signature on the remotely created check.[88]

The drawee bank may also try to pass the loss to the presenting bank or the payee if the drawee bank can demonstrate that the purpose of presenting or transferring the item was part of a scheme to defraud the drawee bank.[89] That, too, is often an unfruitful avenue of recovery in the run-of-the-mill unauthorized drawer's signature case, because the payee and the payee's bank may have no way of knowing that the drawer's signature was in fact not authorized.[90]

c. Recovery Against the Wrongdoer

The last avenue of recovery for the drawee bank is to attempt to recover from the wrongdoer (the unauthorized signor). The drawee bank has the ability to subrogate to the rights of the payee or other holder (including a holder in due course) on the check as against the drawer.[91] As discussed above, that gives the drawee bank rights as against the unauthorized signor, not the purported drawer whose signature was forged.[92]

87. 12 C.F.R. § 229.34(d)(2). This preclusion is broader than the preclusion stated in U.C.C. section 4-406(f) or section 4-208(c). *See supra* note 82.

88. 12 C.F.R. pt. 229, app. E, § XX(D)(1).

89. *See* U.C.C. § 4-302(b) (2005). This "scheme to defraud" exception to the loss resting on the drawee bank is keyed to drawee bank accountability stated in U.C.C. section 4-302(a). As stated in the official comments, drawee bank accountability under U.C.C. section 4-302(a) occurs only if the drawee bank has not made final payment. *Id.* § 3-502 cmt. 4. Final payment is made if the drawee bank preserves its right to return the check and if it fails to return the check by its midnight deadline. *Id.* § 4-215(a)(3). A drawee bank preserves its right to return the check by giving a provisional settlement to the presenting bank by midnight of the banking day of receipt. *Id.* § 4-301(a). Accountability, as opposed to final payment, occurs when the payor bank fails to make a provisional settlement and thus fails to preserve its right to return the item. *See id.* § 3-502 cmt. 4. But because the "scheme to defraud" rule is stated as an exception to the "accountability" rule of U.C.C. section 4-302(a), it is not at all clear that the "scheme to defraud" exception applies if the drawee bank has made final payment instead of becoming "accountable" for the check.

90. *See, e.g.*, Bank of Am. NT & SA v. David W. Hubert, P.C., 101 P.3d 409 (Wash. 2004).

91. U.C.C. § 4-407.

92. *Id.* § 3-403; *see supra* note 45 and accompanying text.

5. Exceptions to the Allocation of Loss to the Payee of the Unauthorized Drawer's Signature if the Check Is Dishonored

If the check is dishonored (generally when timely returned by the drawee bank),[93] the loss based upon an unauthorized drawer's signature will fall on either the payee's bank or the payee. The returned check will eventually be returned to the payee's bank and the payee's bank will charge back the amount of the check against the payee's deposit account.[94] Thus in Example 2, if First Bank dishonored the check, the check will be returned to National Bank and National Bank will charge back the amount of the check against Phil's account.

Phil will then seek to recover from Davis (the purported drawer) based upon the forged drawer's signature on the instrument.[95] Davis will place the unauthorized signature in issue, and then Phil will have to prove that the signature was in fact authorized or that Davis is precluded from asserting the signature was unauthorized.[96] Even if Phil has the rights of a holder in due course on the check, Davis can still assert the defense of an unauthorized signature against Phil. That is because Davis is not liable for the contract obligation on the check unless he signed the check or is precluded from asserting that his signature was not authorized.[97]

The two prime avenues of precluding the purported drawer have already been discussed. Phil could attempt to show that Davis's negligence substantially contributed to the making of the forgery of his signature. If Davis was negligent, Phil was also negligent in taking the check from the wrongdoer, and that negligence substantially contributed to the loss, then comparative loss principles will be used to allocate the loss between Davis and Phil.[98] Phil could also attempt to demonstrate that Davis ratified the wrongdoer's signature.[99] If able to demonstrate that fact, then Phil could recover from Davis on the check. These two avenues of reallocating the loss to Davis (the purported drawer) may not be successful when Phil seeks to recover from the

93. U.C.C. § 3-502(b).

94. *Id.* § 4-214. The payee's bank will suffer the loss in the event that bank is unable to recover from the payee, such as when the payee has insufficient value in its account.

95. *Id.* § 3-414.

96. *Id.* § 3-308.

97. *Id.* §§ 3-401, 3-414. Proof of the signature is part of the prima facie case of the person seeking to enforce contract liability on the instrument and thus forgery of the drawer's signature is failure of an essential element of that prima facie case.

98. *Id.* § 3-406(b); *see supra* notes 59–61 and accompanying text.

99. U.C.C. § 3-403; *see supra* notes 72–73 and accompanying text.

purported drawer on contract liability on the check given the unique factual circumstances that must exist in each situation.[100]

Of course Phil could recover from Francis, the unauthorized signor, as long as Phil took the check in good faith and for value.[101] The unauthorized signature of the drawer operates as the wrongdoer's signature on the check. Thus the wrongdoer, Francis, is the drawer, no matter what name is signed on the drawer's line on the check.[102]

6. Summary of Usual Rules of Loss Allocation Due to an Unauthorized Drawer's Signature

As apparent after this long explanation, the bottom line is that if a check is issued with an unauthorized drawer's signature and the check is paid by the drawee bank, most often, but not always, the drawee bank will be stuck with the loss unless it can recover from the unauthorized signor. If that check is not paid by the drawee bank, most often, but not always, the payee will be stuck with the loss unless it can recover from the unauthorized signor. One of the problems of this scheme is that the above complex set of rules allows for just enough avenues to change that rather simple bottom line based upon peculiar facts and circumstances in any case. This ability to readjust the bottom line risk allocation may encourage a higher cost of allocating this risk than if there were not so many possible permutations for the possible risk allocation.

7. Loss Allocation if Check Truncation

Does this risk-allocation scheme for unauthorized drawers' signatures stay in place if the check collection process is truncated by converting the information from the check to electronic form? Consider the following possible methods for truncation of the check collection process.

One possibility is that the merchant takes the check from the purported drawer, scans the electronic information from the check, inputs the amount, and returns the check to that person. The merchant forwards the electronic information through the banking system to the drawee bank.[103] Assume rather than the merchant scanning the check

100. *See* 6 HAWKLAND & LAWRENCE, *supra* note 78, §§ 3-403:2 [Rev], 3-406:11–:14 [Rev].

101. U.C.C. § 3-403.

102. *See* 6 HAWKLAND & LAWRENCE, *supra* note 78, § 3-403:4 [Rev].

103. *See* Heller, *supra* note 15, at 518 (describing using a check as a source document to create an electronic funds transfer in the ACH network as a debit transaction, but noting that the

for the electronic information, the merchant deposits the paper check to its account at its depositary bank. The depositary bank then scans the electronic information from the check, keys in the amount, and transfers the electronic information through the banking system to the drawee bank.[104]

In order for the risk-allocation rules of Articles 3 and 4 to apply, the check must be a "writing" (Article 3)[105] and an "item" (Article 4).[106] Both of these words have been interpreted to mean a paper format.[107] If the paper format disappears at some point in the process, do Articles 3 and 4 continue to apply? Article 4 allows a small window of opportunity for electronic processing of checks by allowing for banks to make agreements for electronic presentment of items.[108] In essence, the drawee bank would agree to accept presentment of the electronic information from the check instead of insisting on the paper check. Article 4 would continue to apply even though the "item" being presented was now in electronic form. This type of agreement may arise between two or more banks or could take place through clearing-

transaction may result in the information from the check being used to collect through the check network instead of the ACH network).

104. *See id.*, at 518–19, 527–29 (describing the method of either initiating an electronic funds transfer or creating an image to be used in electronic presentment of checks).

105. U.C.C. §§ 3-103(a)(8) (definition of order), 1-201(b)(43) (definition of writing).

106. *Id.* § 4-104(a)(9) (definition of item, referring to an "order"), (c) (incorporating Article 3 definition of "order").

107. *See* Heller, *supra* note 15, at 514–15.

108. U.C.C. § 4-110. Article 4's allowance of electronic presentment does not necessarily mean that the rules from Article 3 that relate to negotiable instruments (which must be in writing) will be applicable to the electronic "item." Some of the rules from Article 3 that have been discussed include the negligence rule in U.C.C. section 3-406, the liability of the drawer under U.C.C. section 3-414, and ratification under U.C.C. section 3-403.

However, if the information from the check is converted to electronic form and then a substitute check is created and presented as authorized under the Check Clearing for the 21st Century Act of 2003 (Check 21 Act), Pub. L. No. 108-100, 117 Stat. 1177 (codified at 12 U.S.C. §§ 5001–5018 (Supp. IV 2004)), arguably Article 4 does not apply at all. There is no provision in Article 4 that allows for truncation to electronics followed by a paper presentment. One of the purported benefits of the Check 21 Act was to speed up the collection process for checks. *See generally* BD. OF GOVERNORS OF THE FEDERAL RESERVE SYS., REPORT TO THE CONGRESS ON THE CHECK CLEARING FOR THE 21ST CENTURY ACT OF 2003, at 4–6 (2007), *available at* http://www.federalreserve.gov/boarddocs/RptCongress/ check21/check21.pdf.

house agreements[109] or by the Federal Reserve Board operating circulars.[110]

In each of the truncation scenarios outlined above, the question is whether the Article 3 and 4 rules govern the allocation of risk from an unauthorized drawer's signature or whether some other set of rules govern that risk allocation once the information is converted from paper form to electronic form. To consider that question fully, the rules regarding funds transfers initiated through non-check mechanisms must first be explored.

B. Credit (Push) Payment Mechanisms: Article 4A

A check is a written order to a bank to transfer value from the payor bank to the payee, regardless of whether the payee is a bank or has an account at another bank. The payee presents that instruction, and so a check payment mechanism is generally considered to be a debit transfer.[111] Now consider a system whereby the payor instructs its bank to transfer value from its account to the account of another person (either at the same bank or a different bank). This is a type of transaction that does not depend upon a written instruction and that requires the payee of the value to have an account at a bank. In fact, the payor's instruction to its bank to transfer funds to the payee's bank account can be given in any manner, including orally or electronically.[112] It is this type of payment mechanism that is covered by U.C.C. Article 4A. For purposes of discussion of Article 4A, assume that no part of the payment transaction is covered by the EFTA and Regulation E.[113] After discussion of Article 4A principles, this section will discuss the application of the EFTA and Regulation E to this type of transaction.

Article 4A applies to credit (push) funds transfers.[114] Article 4A does not cover debit (pull) funds transfers.[115] Funds transfers are de-

109. *See* U.C.C. § 4-110 cmt. 2. For example, a major clearing house offers electronic check presentment services and conducts that business pursuant to agreement among the participating banks. *See* Press Release, The Clearing House Payments Co., SVPCO Image Payments Network Sets New Record (Mar. 8, 2007), *available at* http://www.theclearinghouse.org/press_releases/svpco_2007/002 861.php.

110. *See* U.C.C. § 4-110 cmt. 2; Fed. Reserve Bank, Operating Circular No. 3: Collection of Cash Items and Returned Checks, app. E (July 2006), *available at* http://www.frbservices.org/Operating Circulars/pdf/Oc3.pdf.

111. *See supra* note 10 and accompanying text.

112. U.C.C. § 4A-103(a)(1).

113. *Id.* § 4A-108. *See supra* notes 20–21 and accompanying text.

114. U.C.C. §§ 4A-102, 4A-104, 4A-104 cmt. 4.

fined as a series of payment orders[116] starting with the payor's instructions to its bank to transfer value from its account at the payor bank to the payee by crediting the payee's bank account.[117] The payor who starts the funds transfer is called the originator and the payee is called the beneficiary.[118] The payor bank is called the originator's bank and the beneficiary's depositary institution is called the beneficiary's bank.[119] Sometimes a funds transfer will be simple and involve only the originator's bank and the beneficiary's bank. Often, however, in order to effectuate the transfer of value from the originator to the beneficiary, the originator's bank will issue its own payment order to an intermediary bank and the intermediary bank will issue its own payment order to the beneficiary bank.[120] An originator incurs liability to the originator's bank by issuing a payment order that is accepted by the originator's bank.[121] The originator's bank accepts the originator's payment order when it executes that order by issuing its own conforming payment order either to the beneficiary's bank or an intermediary bank.[122] Similarly, the intermediary bank accepts the payment order of the originator's bank when it executes that order by issuing its own payment order to either another intermediary bank or the beneficiary bank.[123] The beneficiary bank does not issue a payment order, but rather accepts the payment order it receives, generally, by crediting the account of the beneficiary with the amount of the payment order.[124] Upon the beneficiary bank's acceptance of the payment order it received, the originator's obligation to the beneficiary is satisfied to the extent of the amount of the payment order.[125]

115. *Id.* § 4A-104 cmt. 4.

116. A payment order is an instruction to a bank to transfer value from that bank to another bank so as to cause value to be credited to the beneficiary's account at the beneficiary bank. *Id.* § 4A-103(a)(1).

117. *Id.* § 4A-104(a).

118. *Id.* §§ 4A-103(a)(2) (definition of beneficiary), 4A-104(c) (definition of originator).

119. *Id.* §§ 4A-103(a)(3) (definition of beneficiary's bank), 4A-104(d) (definition of originator's bank).

120. *See* U.C.C. 4A prefatory note, § 4A-104(a) (definition of funds transfer), (b) (definition of intermediary bank).

121. *Id.* § 4A-402(c) (the sender of the payment order obliged to pay when receiving bank accepts payment order).

122. *Id.* §§ 4A-209(a) (acceptance of payment order), 4A-301(a) (execution of payment order).

123. *Id.* §§ 4A-209(a) (acceptance of payment order), 4A-301(a) (execution of payment order).

124. *Id.* §§ 4A-209(b), 4A-404, 4A-405.

125. *Id.* § 4A-406(a).

Each payment order creates an independent liability of its sender to the bank that accepted the payment order.[126] The beneficiary bank's acceptance of the payment order it received creates an independent obligation to the beneficiary.[127] These obligations created by issued and accepted payment orders are generally satisfied by a series of debits and credits in bank accounts.[128] For example, the originator's bank generally debits the account of the originator when it accepts the originator's payment order. Assume the originator's bank has an account at the beneficiary bank and the originator's bank sends its payment order (issued to execute the originator's payment order) to the beneficiary bank. When the beneficiary bank accepts the payment order from the originator's bank, the beneficiary bank debits the originator's bank account held by the beneficiary bank and credits the beneficiary's account with the beneficiary bank.[129]

An originator's bank is taking a risk that the originator's payment order is not authorized when it decides to accept the originator's payment order by issuing its own conforming payment order to either the intermediary bank or the beneficiary bank. The general rule is that if the purported originator's payment order was not authorized by the originator pursuant to principles of agency law, the originator is not obligated to pay the amount of that payment order.[130] If the originator's bank then issues its own payment order in execution of the unauthorized payment order, the originator's bank may have to pay its own payment order if the funds transfer is completed by the beneficiary bank accepting the payment order it receives.[131] Because the purported originator, who did not authorize the payment order to the originator's bank, is not liable for the amount of the unauthorized payment order, the originator's bank may not charge the originator's account.[132] In essence, the originator's bank has the liability for having executed a payment order in acceptance of an unauthorized payment order.

The originator's bank may shift the risk of that unauthorized payment order to the purported originator if the originator and the originator's bank have entered into an agreement that the authenticity

126. U.C.C. 4A prefatory note, § 4A-402 cmt. 3.
127. *See id.* § 4A-404.
128. *Id.* §§ 4A-403, 4A-405.
129. *See* MILLER & HARRELL, *supra* note 1, ¶ 10.07.
130. U.C.C. § 4A-202.
131. *Id.* § 4A-402.
132. *Id.* § 4A-202.

of payment orders will be tested with a commercially reasonable security procedure and the bank proves that it accepted the payment order in good faith and in compliance with the security procedure.[133] This rule regarding use of the security procedure is subject to an exception if the originator can prove that the unauthorized payment order was caused by someone who did not obtain access to the information to use the security procedure from the originator or a source controlled by the originator.[134] This exception is not dependent on how the access information was obtained or the originator's failure to exercise any degree of care.[135] If the exception applies, the originator is not liable for the amount of the unauthorized payment order even if the commercially reasonable security procedure was in effect and used by the originator's bank.[136] This set of rules is designed to create incentives for the originator's bank to offer commercially reasonable security procedures and for both the originator and the originator's bank to safeguard information regarding use of the security procedures.[137]

C. Credit or Debit Transfers Involving a Consumer Bank Account: EFTA and Regulation E

Article 4A will not apply to any part of a credit transfer in which a consumer's bank account is debited for a funds transfer which is initiated through an electronic means.[138] Rather, the transaction will be governed by the EFTA and Regulation E.[139] Unlike Article 4A, the EFTA and Regulation E do not address all aspects of the funds transfer. Rather, the focus of the EFTA and Regulation E is on regulation of the relationship between the consumer and the bank holding the consumer's bank account.[140] The EFTA and Regulation E apply to both

133. *Id.* If the customer of the receiving bank has refused a commercially reasonable security procedure and agreed in writing to liability for payment orders sent pursuant to a security procedure the customer designated, that designated security procedure is deemed commercially reasonable. *Id.*

134. *Id.* § 4A-203.

135. *Id.* § 4A-203 cmt. 5.

136. *Id.*

137. 6 HAWKLAND & LAWRENCE, *supra* note 78, § 4A-203:3. The extent to which this risk-allocation scheme can be altered by contract is a matter of some debate. *See* Paul S. Turner, *The UCC Drafting Process and Six Questions About Article 4A: Is There a Need for Revisions to the Uniform Funds Transfers Law?*, 28 LOY. L.A. L. REV. 351 (1994).

138. U.C.C. § 4A-108.

139. *See supra* notes 20–21 and accompanying text. Citations to the EFTA will be to the sections as codified in the United States Code. 15 U.S.C. § 1693a(6) (2000) (definition of "electronic fund transfer"); 12 C.F.R. § 205.3 (2007).

140. 15 U.S.C. § 1693(b); 12 C.F.R. § 205.1(b).

credit and debit transactions involving a consumer's bank account as long as the instruction is initiated through electronic means.[141]

One of the primary regulations of this relationship is the protection of the consumer from liability for unauthorized debits to his or her account. An unauthorized funds transfer is defined as a funds transfer "from a consumer's account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit."[142] A funds transfer is not unauthorized if the consumer furnishes a device used to access the account to the wrongdoer or the consumer is a participant in the wrongdoing.[143]

A consumer will be liable for an unauthorized electronic funds transfer from the consumer's bank account only if the consumer's bank has provided the disclosures required by Regulation E.[144] In addition, if the manner of accessing the consumer's account was an access device,[145] the access device must have been an accepted access device[146] and the bank must have provided a means to identify the consumer to whom it was issued.[147] The paradigm example of an access device is a debit card.[148] An access device may also be a password or code used to access the consumer's bank account information in a web-based format.[149] If those conditions are not met, then the consumer will have no liability at all for the unauthorized electronic funds transfer.[150] Rather, the consumer's depositary bank will bear that risk. This allocation of risk gives the consumer's bank an incentive to provide the disclosures

141. 15 U.S.C. § 1693a(6) (definition of "electronic fund transfer"); 12 C.F.R. § 205.3.

142. 15 U.S.C. § 1693a(11); *see* 12 C.F.R. § 205.2(m).

143. 15 U.S.C. § 1693a(11); 12 C.F.R. § 205.2(m). The regulation provides that a funds transfer is also not unauthorized if the bank holding the account or its employee initiates the debit. 12 C.F.R. § 205.2(m)(3). The official staff commentary to the regulation states, however, "A consumer has no liability for erroneous or fraudulent transfers initiated by an employee of a financial institution." 12 C.F.R. pt. 205, supp. I, § 205.2, cmt. 2(m), note 1.

144. 12 C.F.R. § 205.6(a).

145. An access device is a "card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic funds transfers." 12 C.F.R. § 205.2(a)(1).

146. An access device is "accepted" when the consumer requests, receives, signs, or uses an access device, requests validation of an unsolicited access device, or receives a renewal or substitute access device to replace a previously accepted access device from the same bank. 12 C.F.R. § 205.2(a)(2).

147. 12 C.F.R. § 205.6(a).

148. 12 C.F.R. pt. 205, supp. I, § 205.2, cmt. 2(a), note 1.

149. *Id.*

150. 12 C.F.R. § 205.6(a).

and to provide a means for identifying the consumer authorized to use the access device.

If those conditions are met, then the consumer will be liable for an unauthorized debit to its account in fairly limited circumstances. First, if the access device has been lost or stolen, and the consumer notifies the consumer's bank within two business days after learning of the loss or theft, the consumer's liability is limited to a maximum of $50. The consumer may not be liable even for that amount if the amount of unauthorized transfers that took place before the consumer gave notice to the bank was less than $50.[151]

Second, if the access device is lost or stolen and the consumer does not give notice to the bank within two business days after learning of the loss or theft, the consumer's liability is limited to $500. The consumer's liability could be less than $500 if the amounts of the unauthorized transfers that took place before notice to the bank were less than the $500 maximum and the bank proves that the unauthorized transfers would not have taken place if the consumer had notified the bank within the two business day time period.[152]

Third, if the bank transmits a periodic statement to the consumer, the consumer does not report unauthorized transfers that are on that statement within sixty days of its transmittal to the consumer, and the bank proves that subsequent unauthorized transfers could have been prevented if the consumer had made the report within the sixty days, the consumer will be liable for unauthorized transfers that take place after that sixty day time period.[153] This rule applies regardless of whether there is loss or theft of an access device.[154]

The official staff commentary to Regulation E notes that these risk-allocation rules apply regardless of whether the consumer has been negligent in safeguarding the access device or account information.[155] The bank cannot impose greater liability on the consumer by agreement with the consumer.[156] The time periods noted above can be extended if there are extenuating circumstances, such as the consumer's hospitalization or extended travel away from home.[157]

151. *Id.* § 205.6(b)(1).
152. *Id.* § 205.6(b)(2).
153. *Id.* § 205.6(b)(3).
154. 12 C.F.R. pt. 205, supp. I, § 205.6, cmt. 6(b), para. (6)(b)(3), note 2.
155. 12 C.F.R. pt. 205, supp. I, § 205.6, cmt. 6(b), note 2.
156. 15 U.S.C. § 1693*l* (2000).
157. 12 C.F.R. § 205.6(4).

As briefly noted above, a check may be used to initiate a funds transfer from an account.[158] Recent amendments to Regulation E and its commentary provide that if a check is used as a source document for the information necessary to initiate a funds transfer from the consumer's bank account (generally the routing number and the account number from the Magnetic Ink Character Recognition line, or "MICR line," on the check), Regulation E will cover that transaction.[159] The check is not an "access device," however, so the consumer's liability for unauthorized transfers is limited to the third rule (periodic statement rule) stated above.[160] Regulation E requires that the consumer be given notice that the transaction initiated by check will be processed as a funds transfer instead of through the check collection channel.[161] In some circumstances it may be unclear whether the check is being processed as a funds transfer, covered by Regulation E, as opposed to taking advantage of an electronic presentment agreement with the drawee bank, as allowed by Article 4.[162]

D. Debit or Credit Transfers Governed by System Rules

Funds transfers may be processed through funds-transfer systems as opposed to solely through banks or similar financial institutions. Article 4A defers in some instances to funds-transfer system rules.[163] Article 4A also defers to Federal Reserve System regulations and operating circulars that govern Fedwire, the funds-transfer network run by the Federal Reserve Banks.[164]

One of the most widely used systems for funds transfers is the private network for processing Automated Clearing House (ACH) transactions.[165] Entities that use the system agree to a set of operating rules and guidelines to govern funds-transfer transactions between the entities that are part of the network.[166] Both credit and debit payments are processed through the ACH network.[167] Each transaction

158. *See supra* notes 103–04 and accompanying text.

159. 12 C.F.R. § 205.3(b)(2).

160. 12 C.F.R. pt. 205, supp. I, § 205.2, cmt. 2(a), note 2.

161. 12 C.F.R. § 205.3(b)(2).

162. Heller, *supra* note 15, at 525–29; *see supra* notes 103–10 and accompanying text.

163. U.C.C. § 4A-501(b) (2005). The liability rules for unauthorized transfers as against an entity that is not a bank may not be changed by a system rule. *Id.* § 4A-203 cmt. 7.

164. *Id.* § 4A-107. In Regulation J, the Federal Reserve Board has adopted many of the provisions of Article 4A to govern Fedwire transfers. 12 C.F.R. § 210.25.

165. *See* Heller, *supra* note 15, at 517 n.20.

166. 2007 ACH RULES, *supra* note 16, at ACH Primer 13.

167. *Id.* at ACH Primer 3–4.

starts with an originating depositary financial institution (ODFI) which gives an instruction to either credit or debit an account at the receiving depositary financial institution (RDFI).[168] The ODFI makes warranties for any origination of either a credit or a debit ACH transaction. One of these warranties is that the credit to the receiver's account or debit from the receiver's account is authorized.[169] The ODFI's loss from an unauthorized origination is then allocated to the person that originated the transaction with the ODFI.[170] The ODFI does so through agreement with the originator prior to processing any transactions with the originator.[171] If the transaction is governed by Article 4A (a credit transaction), or by Regulation E, the rules discussed above regarding liability for unauthorized funds transfers cannot be varied by agreement or the funds-transfer system rules.[172]

When a check is truncated during the collection process, the truncation may take place either because it becomes an ACH transaction or because the check is being collected through systems that allow for electronic presentment of items. Recall the discussion of a merchant using the check as a source document, that is, using the MICR line information, keying in the amount, and sending the information to the drawer's bank to debit the drawer's account.[173] Typically, that is a scenario in which the information is being used to initiate an ACH debit transaction from the drawer's bank account. Both Regulation E and ACH rules would generally apply if the debit was from a consumer's deposit account.[174] ACH rules, but not Regulation E, would apply if the debit was from a non-consumer's deposit account.[175] Article 4A would not apply, regardless of the status of the payor, as the transfer is a debit transfer, not a credit transfer.[176] Presumably, the use of the check as a source document is done with notice to the drawer (in ACH terms, the receiver) and at least the implied authorization of the drawer. In a face-to-face transaction, the originator (the merchant) is supposed to have posted notice that the transaction will be processed

168. *Id.*
169. *Id.* §§ 2.2.1.1, 2.2.3, at OR 5–6.
170. *Id.* § 2.1.1, at OR 2; *id.* § 5.3, at OR 23.
171. *See id.* § II, ch. 1, at OG 17 ("Compliance With Security Procedures").
172. U.C.C. § 4A-203 cmt. 7 (2005); 15 U.S.C. § 1693*l* (2000).
173. *Supra* notes 103–04 and accompanying text.
174. *See supra* notes 158–62 and accompanying text. Interestingly, if the ACH payment is transmitted over Fedwire, there is a strong argument that the Regulation E protections for a consumer do not apply. 12 C.F.R. § 205.3(c)(3) (2007).
175. *See supra* note 141 and accompanying text.
176. *See supra* notes 114–15 and accompanying text.

as an ACH transaction.[177] If the truncation of the check happens when the merchant receives the check in the mail, the merchant should have given notice at the time of billing the drawer for the product or services supplied or as part of the agreement with the drawer (such as payment to credit card or utility payees) that all checks would be truncated and turned into ACH debit transactions.[178]

Presumably, in either of these scenarios, the loss allocation principles will be governed by ACH rules and Regulation E, if applicable, and not by the U.C.C. Article 3 and 4 principles discussed above, even though the transaction was initiated using a check. The non-consumer drawer's rights would initially be covered by the agreement it had with its bank (in ACH terms, the RDFI).[179] Assuming the bank account agreement did not accord absolute liability to the non-consumer drawer, the drawer would seek to have the account recredited and the RDFI would recover on the ACH warranties from the ODFI. The ODFI would pass the loss to the merchant initiating the transaction using the check.[180]

In contrast, if the check rules applied, the loss would rest on the RDFI as the check with the unauthorized drawer's signature would not be properly payable from the drawer's account and the RDFI (the drawee) would not be able to recover in most circumstances from the presenting bank (the ODFI, in ACH terms).[181] The check rules would apply if the originally issued check was truncated using agreements for electronic check presentment instead of being converted to an ACH transaction.[182]

E. Debit Transfers Not Governed by EFTA, Regulation E, or System Rules

Assume that a person initiates a pull transaction from a non-consumer account that is not processed through a funds-transfer system (or through Fedwire), so that Article 4A, the EFTA, and system rules do not apply. In this transaction, allocation of the risk of an unauthorized debit to the bank account would be a matter of private

177. *See supra* note 161 and accompanying text; 2007 ACH RULES, *supra* note 16, § II, ch. 1, at OG 38.

178. 2007 ACH RULES, *supra* note 16, § II, ch. 1, at OG at 38–39.

179. *See supra* notes 168–69 and accompanying text; 2007 ACH RULES, *supra* note 16, § II, ch. 4, at OG 76–77.

180. *See supra* notes 169–71.

181. *See supra* notes 51–53 and accompanying text.

182. *See supra* notes 108–10 and accompanying text; Heller, *supra* note 15, at 524 n.57.

agreement between the participants in the system. An example of this situation would be where Person A, a non-consumer account holder at Bank A, has Bank A issue an instruction to Bank B to debit the account of non-consumer account holder, Person B, and credit the account of Person A at Bank A. Assuming Person A is acting without the actual authorization of Person B, Person A is likely to have some sort of forged authorization that would purportedly demonstrate to both Bank A and Bank B that Person A was authorized to pull the funds from Person B's account. If Bank A and Bank B executed those instructions without using any funds-transfer system, such as ACH, the allocation of the risk of Person A not being authorized would likely be determined by the bank-customer agreement between Person B and Bank B and indemnity arrangements between Bank A and Bank B.

II. PRINCIPLES FOR RISK ALLOCATION OF UNAUTHORIZED PAYMENT INCEPTION

Does it have to be so complicated? Are the rules used to allocate the risk of this type of fraud sensible in terms of the policies that should be advanced? One of the benefits of an exercise of imagination is the ability to look beyond the status quo and ask this question: if we could design a system of legal rules today that would allocate the risk of unauthorized debits to a deposit account, what considerations and principles should we take into account in designing those rules?[183] This exercise in imagination should not be tethered to how it has always been done, but rather should be a free-ranging inquiry as to whether there is a better way to allocate the risk than under current law.[184] When judging whether there is a "better" way, it is essential to

183. The New Payments Code project of the National Conference of Commissioners on Uniform State Laws and the American Law Institute was an example of one attempt to engage in this more unified process. That project failed in part in the early 1980s, but out of that process U.C.C. Article 4A was developed, and a much smaller revision project of U.C.C. Articles 3 and 4 was undertaken. *See generally* Gregory E. Maggs, *New Payment Devices and General Principles of Payment Law*, 72 NOTRE DAME L. REV. 753, 773–75 (1997); Fred H. Miller, *A Report on the New Payments Code*, 39 BUS. LAW. 1215 (1984); Fred H. Miller, *U.C.C. Articles 3, 4 and 4A: A Study in Process and Scope*, 42 ALA. L. REV. 405 (1991); Carlyle C. Ring, Jr., *The UCC Process—Consensus and Balance*, 28 LOY. L.A. L. REV. 287 (1994); Hal S. Scott, *Corporate Wire Transfers and the Uniform New Payments Code*, 83 COLUM. L. REV. 1664 (1983); James V. Vergari, *A Critical Look at the New Uniform Payments Code*, 9 RUTGERS COMPUTER & TECH. L.J. 317 (1983); Note, *Consumer Protection and Payment Systems: Regulatory Policy for the Technological Era*, 98 HARV. L. REV. 1870 (1985); Note, *Overcoming the Obstacles to Implementation of Point-of-Sale Electronic Fund Transfer Systems: EFTA and the New Uniform Payments Code*, 69 VA. L. REV. 1351 (1983).

184. Payments law has been the subject of recent commentary regarding whether the risk-allocation rules make sense in the modern environment with the proliferation of payment mechanisms. *See, e.g.*, Mark E. Budnitz, *Consumer Payment Products and Systems: The Need for*

ask what objectives should guide the conclusion that a new way is "better" than the current methods.[185]

In evaluating any objectives that are considered for building[186] a better risk-allocation system, one of the guiding considerations has to be balancing the costs of operating the system as it is, including the cost of unauthorized debit risk allocation, against the cost and feasibility of implementing new legal rules that would change that risk allocation in order to create incentives to reduce the amount of losses

Uniformity and the Risk of Political Defeat, 24 ANN. REV. OF BANKING & FIN. L. 247 (2005) [hereinafter Budnitz, *Consumer Payment Products*]; Mark E. Budnitz, *Stored Value Cards and the Consumer: The Need for Regulation*, 46 AM. U. L. REV. 1027 (1997); Ronald J. Mann, *Making Sense of Payments Policy in the Information Age*, 93 GEO. L.J. 633 (2005); Ronald J. Mann, *Searching for Negotiability in Payment and Credit Systems*, 44 UCLA L. REV. 951 (1997); James Steven Rogers, *The Irrelevance of Negotiable Instruments Concepts in the Law of the Check-Based Payment System*, 65 TEX. L. REV. 929 (1987); James Steven Rogers, *The Myth of Negotiability*, 31 B.C. L. REV. 265 (1990); James Steven Rogers, *The New Old Law of Electronic Money*, 58 SMU L. REV. 1253 (2005).

This inquiry should also not ignore the international aspect of payments law. *See generally* Carl Felsenfeld, *The Compatibility of the UNCITRAL Model Law on International Credit Transfers with Article 4A of the UCC*, 60 FORDHAM L. REV. (COLLOQUIUM) S53 (1992); Mark Sneddon, *The Effect of Uniform Commercial Code Article 4A on the Law of International Credit Transfers*, 29 LOY. L.A. L. REV. 1107 (1996).

This article does not address issues concerning the enforcement of criminal laws, such as anti-money laundering regulation. *See, e.g.*, FINANCIAL ACTION TASK FORCE, REPORT ON NEW PAYMENT METHODS (2006), *available at* http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf.

185. For an argument that the funds-transfer system should serve the purpose of effective functioning of the financial markets, see Raj Bhala, *The Inverted Pyramid of Wire Transfer Law*, 82 KY. L.J. 347 (1993); Steven B. Dow & Nan S. Ellis, *The Proposed Uniform New Payments Code: Allocation of Losses Resulting from Forged Drawers' Signatures*, 22 HARV. J. ON LEGIS. 399 (1985) (critiquing the change in loss allocation for forged drawer's signature as proposed in the new payments code, arguing that the payor bank will have no incentive to try and avoid the loss under the proposed rules).

186. Part of the challenge of building a better payment system is figuring out the appropriate mechanism for drafting the risk-allocation rules. Just what process would be best to construct a more functional set of risk-allocation rules is a matter of debate. When the New Payments Code failed and the 1990 revisions of U.C.C. Articles 3 and 4 were promulgated, there was widespread criticism and defense of the uniform laws process concerning the degree to which the changes were perceived as being too "industry friendly." *See, e.g.*, Mark E. Budnitz, *The Revision of U.C.C. Articles Three and Four: A Process Which Excluded Consumer Protection Requires Federal Action*, 43 MERCER L. REV. 827 (1992); Kathleen Patchel, *Interest Group Politics, Federalism, and the Uniform Laws Process: Some Lessons From the Uniform Commercial Code*, 78 MINN. L. REV. 83 (1993); Donald J. Rapson, *Who is Looking Out for the Public Interest? Thoughts About the UCC Revision Process in the Light (and Shadows) of Professor Rubin's Observations*, 28 LOY. L.A. L. REV. 249 (1994); Edward Rubin, *Efficiency, Equity and the Proposed Revision of Articles 3 and 4*, 42 ALA. L. REV. 551 (1991); Edward L. Rubin, *Thinking Like a Lawyer, Acting Like a Lobbyist: Some Notes on the Process of Revising UCC Articles 3 and 4*, 26 LOY. L.A. L. REV. 743 (1993).

When Congress enacted the Check 21 Act in 2003, see *supra* note 108, there was criticism of that law from the perspective of the uncertainties it created for rights and liabilities concerning substitute checks. *See, e.g.*, Carl Felsenfeld and Genci Bilali, *The Check Clearing for the 21st Century Act—A Wrong Turn in the Road to Improvement of the U.S. Payments System*, 85 NEB. L. REV. 52 (2006); Mark Hargrave, C*heck 21: A Year in the Life*, 38 UCC L.J. 233 (2006).

incurred.[187] If a new set of rules would help prevent losses without significant increase in transaction costs, the system as a whole could function more efficiently, thus better facilitating economic activity.[188]

Another objective should be the clear allocation of risk in a transparent set of rules whereby the system participants know what risks they are taking on in using the system.[189] The current diversity in risk-allocation rules depending on the mechanism used, the method of processing, and the type of deposit account held, is anything but transparent and clear. That lack of transparency imposes a cost on the system of transferring value.

A. Risk Spreading

Consider one possible objective for revision of the risk-allocation rules of unauthorized debits to a deposit account: allocate the loss of unauthorized debits to the person in the best position to spread the loss among all the players in the payment system.[190] If this objective was the primary focus, the typical entities that could spread the loss among payment system players would be the payor bank or the payee's bank.[191] Either of those entities could price their services based upon a certain predictable percentage of losses from unauthorized debits and, through pricing, spread those losses.[192] If risk spreading was the policy basis, the rule for risk allocation for an unauthorized debit could be relatively simple. For example:

187. *See* BIS, *supra* note 3, § 3.3.1, at 6 ("A system's rules and procedures should therefore ensure that all parties have both the incentives and the capabilities to manage and contain each of the risks they bear and that limits are placed on the maximum level of credit exposure that can be produced by each participant."); *id.* §§ 7.8.16–.19, at 47; Clayton P. Gillette, *Rules, Standards, and Precautions in Payment Systems*, 82 VA. L. REV. 181, 221 (1996). *See, e.g.*, Raj Bhala, *Paying for the Deal: An Analysis of Wire Transfer Law and International Financial Market Interest Groups*, 42 U. KAN. L. REV. 667, 669–70 (1994) (assessing risks based on economic principles and banking system concerns to determine whether payment system rules strike the right balance).

188. *See* Bhala, *supra* note 185, at 377–78 (focusing on large dollar value funds transfers in sophisticated financial markets). Whether the payment system should be structured to provide access for persons of more limited means is an interesting policy issue. *See* Michael S. Barr, *Banking the Poor*, 21 YALE J. ON REG. 121 (2004).

189. *See* FEDERAL RESERVE POLICY ON PAYMENTS SYSTEM RISK, *supra* note 1, at 11; BIS, *supra* note 3, § 3.2.1, at 6 ("Participants . . . should understand clearly the financial risks in the system and where they are borne."). *But see* Budnitz, *Consumer Payment Products*, *supra* note 184, at 278 (arguing that consumers should have a uniform rule for all payment products but should not have more liability than what they currently have for unauthorized payment inceptions).

190. Robert D. Cooter & Edward L. Rubin, *A Theory of Loss Allocation for Consumer Payments*, 66 TEX. L. REV. 63, 71–72 (1987).

191. *See id.* at 72.

192. *Id.*

> A financial institution may debit its customer's account only for amounts authorized by its customer. A debit is authorized by the customer only if the customer actually authorized the debit or is bound to the authorization under principles of agency law. This rule may not be altered by agreement between the customer and the financial institution.

This rule would allocate the risk of an unauthorized debit to the depositary institution holding the deposit account. The only factual dispute would be "authorization."

The difficulty with this approach is that it does not take into account whether there are any opportunities for loss prevention. While not all unauthorized debits can be prevented, the cost of unauthorized debits to the payment system as a whole should not be underestimated.[193] A loss spreading rationale would accept the level of unauthorized debits as a cost of doing business and would not necessarily foster any incentives or realistic opportunities to decrease the cost of operating the payment system as a whole. Using the rule given above as an example, the customer would not have any incentive to safeguard its account information or monitor its account transactions. The payor bank would take the risk for its customer's behavior with very little ability to control that risk.

Structuring a rule that would make the payee's bank the risk spreader is somewhat problematic. A possible rule is as follows:

> A paying bank may recover from a payee bank if the payee bank obtained credits from the paying bank based upon an unauthorized debit from the account of a customer of the paying bank. A debit is authorized by the customer of the paying bank only if the customer actually authorized the debit or is bound to the authorization under principles of agency law. A payee bank that is obligated to the paying bank for the amount of the credit may not deduct the recovered credit from its customer's account. This rule may not be altered by agreement.

Placing the loss on the payee's bank further divorces risk prevention from risk bearing unless one presumes that the payee is the bad actor, and the rule creates an incentive for the payee's bank to "know its customer." Even having said that, placing the risk on the payee's bank to further loss-spreading principles does not give the payee bank any mechanism for protecting against the loss without extensive

193. *See, e.g.*, BD. OF GOVERNORS OF THE FEDERAL RESERVE SYS., A SUMMARY OF THE ROUNDTABLE DISCUSSION ON RETAIL PAYMENTS FRAUD (2007), *available at* http://www.federalreserve.gov/paymentsystems/retailpmtfraud/retailpmtfraud.pdf.

screening and ongoing monitoring of its customer's business practices. That monitoring also increases the cost of this risk-allocation rule.

B. Certainty of Result of Risk Allocation and Finality of Payment

Another objective for allocating the risk of fraudulent payment inceptions could be creating certainty of result, that is, a clear rule that allocated the risk to a player in the system so that player would know that if the risk happened that person would bear the risk. This would ultimately encourage the risk bearer to take what the risk bearer perceived as adequate precautions to either prevent the risk from happening or to insure against the risk if it happened in spite of precautions. If certainty of result was the only objective, it would not matter who the player was that bore the risk (the payor, the payor bank, the payee, the payee's bank, or an intermediary bank), as long as the result was clear.[194] It would be that designated risk taker's problem.

Another objective that could be pursued that is closely related to certainty of result is the protection of finality of payment. That is, if there is a debit from the account, even if unauthorized, the finality of that payment should be respected and the ability to reverse that transaction (and allocate the loss to someone other than the payor or the payor bank) should not be allowed.[195] Finality of payment allows for protection of payees and intermediaries in the system that may not be able to determine that the purported payor's instruction to the payor bank was unauthorized. Finality of payment principles encourages use of a payment system.[196] For instance, currency transactions have a very strong finality principle. Other than the ability to recover currency from the person who stole it from the currency owner, transferees of currency for value and without notice that the currency is stolen are

194. *Cf.* Rogers, *supra* note 7, at 467 (arguing that "unpreventable" losses should be born by the providers of the system (the banks) and not the users of the system).

195. *See generally* Jane Kaufman Winn, *Clash of the Titans: Regulating the Competition Between Established and Emerging Electronic Payment Systems*, 14 BERKELEY TECH. L.J. 675, 679 (1999) (finality is essential to a functioning payment system). There is an argument that finality of payment should bow to the user's ability to stop payment so as to enable the user to exercise leverage in the underlying transaction. *See generally* Raymond T. Nimmer, *Consumer Payment Systems: Leverage Effects Within an Electronic Funds Transfer System*, 17 HOUS. L. REV. 487 (1980).

196. *See* Bhala, *supra* note 185, at 385–89. A closely related issue is the ability to control systemic risk that may result to the payment system as a whole if payments are not cleared in a timely manner and transactions could be unwound if a participant was unable to clear the payment. *Id.* at 390–93. *See generally* BD. OF GOVERNORS OF THE FEDERAL RESERVE SYS., FEDWIRE FUNDS TRANSFER SYSTEM: ASSESSMENT OF COMPLIANCE WITH THE CORE PRINCIPLES FOR SYSTEMICALLY IMPORTANT PAYMENT SYSTEMS (rev. ed. 2006), *available at* https://www.federalreserve.gov/paymentsystems/coreprinciples/ coreprinciples.pdf.

protected from the currency owner's claim that the currency should be returned to the owner.[197] The finality of the transaction between the innocent taker for value and the person it dealt with is more important than the property-based claim of the rightful owner to the currency. This rule is often justified as essential to a monetary, as opposed to a barter, payment system because it encourages acceptance of the monetary token.[198]

Certainty of result and finality of payment as objectives would cut down the transaction costs of a risk-allocation system that placed the risk on other parties in a manner that depended upon the facts and circumstances of an individual case.[199] This reduction of cost in operating the payment system would be a significant benefit of a rule that placed the liability on a designated risk taker in all circumstances in order to protect the finality of a payment once made. The rule given above, which places the loss on the payor's institution, creates a certain result and respects finality of payment. The rule placing the risk on the payee bank, while creating a certain result, does not respect finality of payment principles.

Certainty of result and finality of payment cannot be the only objectives. For one thing, if the designated risk taker could not do anything to prevent the risk, in essence the system would be treating the designated risk taker as an insurer of the system. In order for the designated risk taker to be agreeable to taking on that risk,[200] the risk taker would need some form of compensation for that risk, just as an insurer is compensated through premium payments for taking on risks that it cannot prevent. This insurance-orientated principle may create a separation between the entity that bears the costs and the entity that may be able to prevent the costs.[201] That separation is expensive for a payment system, as it may not lead to reduction in this type of risk at all. Thus, if the payor bank must always take the loss, the payor, or other parties in the system, may lose any realistic incentive to try to prevent the loss. The payor bank may also implement loss-prevention principles that would unduly burden the functioning of the system or

197. *See* City of Portland v. Berry, 739 P.2d 1041 (Or. Ct. App. 1987).

198. *See id.* at 1044.

199. Cooter & Rubin, *supra* note 190, at 78.

200. This is after all a process about enacting law, a political process where stake holders are not inactive.

201. This is often referred to as a moral hazard that is often associated with policy analysis regarding where the loss should be placed in discussions of tort law. *See generally* Tom Baker, *On the Genealogy of Moral Hazard*, 75 TEX. L. REV. 237 (1996).

price its services at a cost that makes the payment system uneconomical for use, in order to compensate itself for taking the risk of losses that another party might have had the ability to prevent, to the detriment of the overall economic system that payments supports.

C. Best Position to Prevent the Loss

Perhaps the objective of the risk-allocation rules for unauthorized debits to a deposit account should not be randomly allocated to any player in the system, but rather the risk should fall on the player in the best position to protect against the unauthorized debit.[202] Given the structure of deposit accounts, the two most likely risk holders using this principle are the payor and the payor bank. All of the other players in the system are not in a position to evaluate the authenticity of instructions directed at a deposit account, that is, whether the payor really authorized the debit from the account. A rule that allocates the risk of authenticity to the payor bank was already given above. A rule that would allocate the risk of authenticity to the payor could be as follows:

> A financial institution may debit its customer's account for an authorized or an unauthorized debit.

Are either the payor or the payor bank (or both) in a position to evaluate the authenticity of the payor's instruction directly to the payor bank (a credit transfer), or funneled through the payee (a debit transfer)? Is that a viable premise as a matter of factual reality?

Consider the payor bank. A check is written purportedly signed by the drawer. Under current banking standards and processing methods, it is not feasible for someone at the payor bank to actually determine if the signature on the check is in fact that of the purported drawer. Even if it was cost effective to have an actual person examine the signatures, the ability for that person, even if qualified as a handwriting expert, to make sure that the signature on the check matches the signature on the account's signature card is purely fictional. Now consider a funds transfer from the payor's account in which a plastic card is used at a point-of-sale terminal to initiate the debit. Is it feasible for the payor bank to determine if the person actually using the card is in fact the payor or someone that the payor authorized to use the card? Additional codes, such as a PIN, may be required, but that is no guarantee that the payor authorized the usage. Biometrics such as thumbprints,

202. Cooter & Rubin, *supra* note 190, at 73–75.

eye scans, or other biological indicators could be input and sent along with the payment information.[203] Current technology may not be capable of handling that data either at the inception end or at the payor bank's processing facilities. In addition, that sort of data collection may raise privacy concerns.[204]

Now consider whether the payor is in a position to evaluate the authenticity of the instruction to debit the account. The payor does not have ready access to the information that the payor bank receives when an instruction is given to that bank to debit the payor's account. Therefore, in order for the payor to evaluate the instruction to debit the account, the payor bank would have to contact the payor to determine whether the instruction was authentic. Should the system rule require that before any debits are made, the payor is contacted for specific authorization? While this would probably cut down on the number of unauthorized debits, the cost of this approach would be significant and the speed of payment clearance would be seriously undermined.

Should the system rules instead require the payor to notify the payor bank anytime a payment has been authorized, so the bank would know that when the payment came into the bank's system the instruction to debit the account should be followed? While that system is likely to be less expensive than an individualized contact with each payor as instructions are received by the bank, it also is not a fail-safe system. How would the payor bank know that the purported payor giving the advance approval is in fact the authorized payor? Some sort of authentication procedure would have to be in place. How would this type of system deal with transactions that are not planned in advance, such as the Sunday shopping expedition where the purported payor is making purchases and payment instructions are transmitted from the point of sale? Should the payor have to present himself or herself physically at the payor bank to withdraw credits from the deposit account?

If the payor is expected to evaluate the authenticity of instruction to debit the account, should the relative sophistication of the payor be taken into account? Should the payor who is an individual consumer be held to a different standard for verifying authenticity than a multinational, billion-dollar corporation?

203. *See id.* at 76–77 (noting that technology might be able to reduce losses).

204. *See generally* Shane L. Smith, *Gone in a Blink: The Overlooked Privacy Problems Caused by Contactless Payment Systems*, 11 MARQ. INTELL. PROP. L. REV. 213 (2007).

Instead of thinking that the loss has to be either totally on the payor bank or on the payor, consider whether the system rules should encourage the payor to safeguard its information concerning instructions to the payor bank and the payor bank to provide mechanisms to assist the payor in that regard. Of course, to the extent that the rules rely on too many factual determinations in a specific case, that will increase the transaction costs related to allocation of the loss.[205]

In considering rules that would focus on the payor's efforts to safeguard the information for giving the instruction, several different options are possible. One option could be an "ordinary care" rule, that is, the payor has the obligation to use ordinary care in safeguarding the information used to instruct the payor bank to debit the payor's account. The payor would be liable for any unauthorized debit in which it was demonstrated the payor failed to use ordinary care. An example of such a rule is as follows:

(1) A financial institution may debit a customer's account only if:
    (a) The debit is authorized by the customer; or
    (b) The debit is unauthorized and the customer's failure to use ordinary care resulted in the unauthorized debit.
(2) A debit is authorized by the customer only if the customer actually authorized the debit or is bound to the authorization under principles of agency law.

This option does not offer any incentive for the payor bank to offer mechanisms to assist the payor in safeguarding access to the account, nor does it take into account any steps that the payor bank should take on its own to be sure it is acting on authorized instructions. To take into account the payor bank's actions, one could use a comparative or contributory negligence analysis to determine who is more "at fault" in allowing the unauthorized payment. Inquiry into either the payor's or the payor bank's failure to act with ordinary care is a factually uncertain and potentially expensive inquiry.[206] Is the expense and uncertainty worth the effect it may have on encouraging incentives to prevent loss due to an unauthorized debit? Can advice be given with a relative level of confidence that if these precautions are taken, the relevant actor has acted with ordinary care? In addition, does the "ordinary care" standard set the right standard of behavior? Perhaps merely being not negligent is not a sufficient level of incentive

205. Cooter & Rubin, *supra* note 190, at 78–84.
206. *Id.*

to take care given the structure of modern banking and the electronic communication environment.

Allocation of the risk of unauthorized payments between the payor and the payor bank could be made more certain, that is, not dependant upon a standard such as the lack of ordinary care. One way to split the risk, but not hinge it to a factual inquiry, is to limit the ability to debit the payor's account based upon some percentage of the amount of the unauthorized instruction. The percentage could be mandated at a fixed point or it could float based upon some external scale, such as the value of all amounts on deposit with that institution, the average value of a transaction, or the average volume of transactions. The key to fixing the percentage would be to attempt to predict what level of risk sharing would lead to the optimal level of precautions against the unauthorized debit.[207] A possible articulation of this type of rule could be:

> A financial institution may debit its customer's account for XXXX% of the amount of an unauthorized debit. A debit is unauthorized if the customer did not actually authorize the debit or is not bound to the authorization under principles of agency law. This rule may not be altered by agreement.

This percentage could be very difficult to fix at the optimal level and there is no empirical data that would be very helpful in picking what the right level of risk sharing is. Any percentage would thus be somewhat arbitrary. Arbitrariness, however, is cheaper than factual inquiry regarding ordinary care.

Another approach is to encourage the payor and the payor bank to put into place security procedures by which authenticity could be verified at the time the payor bank received the instruction to debit the account. A possible rule using this approach is as follows:

> A financial institution may debit a customer's account only if:
>
> (a) the customer actually authorized the debit or is bound by the authorization under the law of agency; or
>
> (b) the customer and the financial institution have agreed to use a commercially reasonable security procedure to verify the authenticity of the debit and the financial institution complied with the procedure to authenticate the debit instruction.

207. Alternatively, the payor's liability could be fixed at a capped amount, as in the credit card rules. *See* 12 C.F.R. § 226.12(b) (2007). Setting the optimal level of the cap could be as difficult as setting the optimal percentage, as stated in the text. *See* Cooter & Rubin, *supra* note 190, at 97.

Similar to the rule in Article 4A,[208] this rule places an incentive on the financial institution to offer commercially reasonable security procedures. As noted in the comment to Article 4A:

> 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. . . . 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.[209]

Focusing on the commercial reasonableness of the security procedure allows usage of banking standards and available technology to factor into what is a commercially reasonable security procedure. It also allows the relative sophistication of the payor and the payor bank's process to factor into what is commercially reasonable for that payor.[210] That inquiry should be more predictable than an inquiry into whether either the payor or the payor bank exercised ordinary care. What this rule does not do is place much incentive on the payor to agree to use the procedure.

Thus perhaps the rule should more closely resemble the rule in Article 4A, that is, it should create an incentive on the payor bank to offer commercially reasonable security procedures and an incentive on the payor to agree to and use those commercially reasonable security procedures. Article 4A encourages the payor to agree to the use of commercially reasonable security procedures by deeming the security procedure the customer agrees to use as commercially reasonable if the bank offers and the customer refuses a commercially reasonable security procedure, and the customer agrees to be bound by a payment

208. U.C.C. § 4A-202 (2005).

209. *Id.* § 4A-203 cmt. 1.

210. Article 4A defines a commercially reasonable security procedure as follows:

> 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.

Id. § 4A-202(c).

order sent pursuant to the customer's chosen security procedure.[211] If the customer will not agree to take on the liability from use of its chosen security procedure instead of the commercially reasonable security procedure offered by the bank, the bank, in all likelihood, will refuse to conduct funds transfers for the customer. As stated in the official comments to Article 4A:

> The purpose . . . is to encourage banks to institute reasonable safeguards against fraud but not to make them insurers against fraud. . . . 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.[212]

To encourage both the payor and the payor bank to use commercially reasonable security procedures, the rule proposed above could be restated as follows:

> A financial institution may debit a customer's account only if:
>
> (a) the customer actually authorized the debit or is bound by the authorization under the law of agency;
>
> (b) the customer and the financial institution have agreed to use a commercially reasonable security procedure to verify the authenticity of the debit and the financial institution complied with the procedure to authenticate the debit instruction; or
>
> (c) the customer refused to agree to use a commercially reasonable security procedure offered by the financial institution to verify the authenticity of the debit instruction.

This rule also should operate to put incentives on the customer to safeguard the means of complying with the security procedure. As stated in the comments to Article 4A:

> 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.[213]

Unlike Article 4A, this proposed rule does not shift the loss to the payor bank if the customer can prove that the means of breaching the security procedure was obtained from a source other than the customer.[214] The most likely source of the information to breach the security procedure, other than the customer, is one controlled by the

211. *Id.* § 4A-202(c).
212. *Id.* § 4A-203 cmt. 4.
213. *Id.* § 4A-203 cmt. 5.
214. *Id.* § 4A-203(a)(2).

financial institution.[215] If that sort of exception applied, it would also encourage the financial institution to safeguard the information concerning the security procedure. Thus the proposed rule could be altered as follows:

> (1) Except as provided in subsection (2), a financial institution may debit a customer's account only if:
>
> (a) the customer actually authorized the debit or is bound by the authorization under the law of agency;
>
> (b) the customer and the financial institution have agreed to use a commercially reasonable security procedure to verify the authenticity of the debit and the financial institution complied with the procedure to authenticate the debit instruction; or
>
> (c) the customer refused to agree to use a commercially reasonable security procedure offered by the financial institution to verify the authenticity of the debit instruction.
>
> (2) A financial institution may not debit its customer's account under subsection (1)(b) if the information facilitating breach of the commercially reasonable security procedure was not obtained directly or indirectly from the customer.

This loss allocation scheme thus provides a clear, transparent, and functional rule in which there are limited questions that must be resolved as a matter of particular facts. The factual uncertainties would be whether the debit was actually authorized or the customer was bound to the communication by agency law, whether the security procedure was commercially reasonable, whether the bank complied with the security procedure, and whether the wrongdoer obtained information used to breach the security procedure from the purported payor.

Would this loss allocation rule work for the payment mechanisms that are not currently Article 4A transactions, such as checks, pull (debit) funds transfers, and consumer electronic funds transfers subject to the EFTA and Regulation E?

Part of the challenge of adapting the Article 4A model to the current payments environment is the psychological hurdle that requires an acknowledgment that, just as with Article 4A payment orders, the processing of debits against the payor's deposit account is conducted through automated systems without human involvement, regardless of the mechanism used to initiate the debit. Payor banks do not routinely examine the signature of the drawer on checks to determine if the

215. *See id.*

check is an authorized order of the drawer.[216] Checks are processed by automated means using the MICR line information. Electronic funds transfers from accounts through point-of-sale purchases, ATMs, or other mechanisms are not examined to determine if the consumer is in fact ordering the debit. Those funds-transfer systems already depend upon algorithms or other security procedures such as PIN numbers to determine some level of authenticity.[217]

Another level of analysis must be to consider a policy choice in the case of a consumer deposit account. The policy question is whether in regard to a consumer transaction, the consumer should be charged with safeguarding the security procedure information. Under current Regulation E, the consumer has no incentive (from a liability standpoint rather than an inconvenience standpoint) to safeguard the access information.[218] Is this the right policy choice? Does that perspective lead to an insufficient level of caretaking to reduce the amount of loss from unauthorized transactions?

Once one acknowledges the automated and computer assisted payment processing environment when an instruction is presented to a payor bank to debit an account and the need to reconsider the consumer protection policy for consumer accounts, then the remaining challenge is an operational one. Can the payor bank institute the necessary processing capability to offer commercially reasonable security procedures for all types of mechanisms used to initiate debits from a deposit account? It is easiest to imagine such security procedures being possible if the instruction to debit an account is communicated electronically to the payor bank. In that circumstance, it is a matter of programming to add information to the electronic communication that would result in the ability to verify the communication pursuant to a defined security procedure.

The old-fashioned paper check presents the hardest case for imagining commercially reasonable security procedures that could be instituted to verify the authenticity of the check as one issued by the drawer.[219] The security procedure would have to consist of some cod-

216. *See supra* note 61 and accompanying text.

217. *See generally* BD. OF GOVERNORS OF THE FEDERAL RESERVE SYS., A SUMMARY OF THE ROUNDTABLE DISCUSSION ON THE RISK AND SECURITY INVOLVING RETAIL PAYMENTS OVER THE INTERNET (2005), *available at* http://www.federalreserve.gov/paymentsystems/internetpayments/ default.htm.

218. *See* 12 C.F.R. pt. 205, supp. I, § 205.6, cmt. 6(b), note 2 (2007) ("consumer behavior that may constitute negligence under state law, such as writing the PIN on a debit card or on a piece of paper kept with the card, does not affect the consumer's liability for unauthorized transfers").

219. Although the check's demise has been oft predicted, and its use has been declining, it still represents a significant percentage of the payments market. *See* Geoffrey R. Gerdes, Jack K.

ing added to the check by the drawer at the time of issuance, not when the checks are preprinted with the payor bank's identifying code, the account number and check number. That coding would have to be recognizable by the payor bank's automated processing system. That coding would also have to be something that would not be readily apparent to the payee or other parties that may handle the check prior to the presentment to the payor bank; otherwise, that coding information could be readily used to breach the security procedure. Whether that type of coding is possible must be addressed before one would seek to apply this proposed rule to old-fashioned paper checks.[220]

If such coding was not possible and the proposed rule applied to all payments except old-fashioned paper checks, payor banks perhaps would price check services sufficiently to account for the losses from unauthorized debits based upon an unauthorized drawer's signature. If the pricing reflected the real degree of risk to the payor bank, perhaps this would continue the demise of the paper-based transaction.

CONCLUSION

As has been demonstrated, imagining rules that change the current balkanized scheme of loss allocation due to unauthorized payments inceptions involves identifying the policies that are desired, crafting rules that advance those policies, and then determining whether the implementation of those policies is operationally possible given the current state of technology. This approach allows for a more instrumental mode of considering payments mechanisms as tools to facilitate economic activity and allows a more realistic methodology in structuring the costs of providing those mechanisms.

Walton II, May X. Liu & Darrel W. Parke, *Trends in the Use of Payment Instruments in the United States*, FED. RES. BULL., Spring 2005, at 180, 181 (although check usage declined from 2000 to 2003, checks still represented the largest non-cash payment method); FEDERAL RESERVE SYSTEM, THE 2007 FEDERAL RESERVE PAYMENTS STUDY: NONCASH PAYMENT TRENDS IN THE UNITED STATES: 2003–2006, at 5–9 (2007), *available at* http://www.frbservices.org/files/communications/pdf/research/2007_payments_ study.pdf.

220. One could imagine in a point-of-sale transaction where a check is used as a source document to initiate an ACH transaction that the drawer would also have to input a PIN number (or other security algorithm) that the merchant would not have access to. This would not work, however, if the check was truncated at a point later than the point of sale.