

## UNIFORMITY AND DIVERSITY IN PAYMENT SYSTEMS

CLAYTON P. GILLETTE\* AND STEVEN D. WALT\*\*

## INTRODUCTION

Current law adopts different rules for different payment systems. The allocation of losses from unauthorized payment, erroneous payment, and the reversibility of instructions to pay varies depending on whether payment is made by check, credit or debit card, wholesale wire transfer, or letter of credit.<sup>1</sup> On its face, the diversity of payment systems rules seems counterproductive. It can cause confusion among users of payment systems, who might assume that rules with which they are familiar from one system apply similarly to other systems. Diversity thus increases learning costs among users and leads to unanticipated consequences when uninformed users make incorrect assumptions about uniformity. The greater the degree of uniformity across payment systems, the lower the search costs incurred by a party in selecting the appropriate device for her transaction. Diversity also often appears to be a consequence of historical contingency rather than well-designed analysis. To take a minor example, it is difficult to reconcile the different statutory definitions for “unauthorized” credit cards and consumer electronic fund transfers other than by reference to drafting inconsistencies over time.<sup>2</sup> Finally, the costs of diversity

\* Max E. Greenberg Professor of Contract Law, New York University School of Law. Thanks to Oren Bar-Gill and Ronald Mann for insightful comments on earlier drafts.

\*\* Professor of Law and Sullivan & Cromwell Research Professor, University of Virginia School of Law.

1. Rules applicable to particular payment devices also vary across countries. See BENJAMIN GEVA, *BANK COLLECTIONS AND PAYMENT TRANSACTIONS* 210–18 (2001) (wire transfer law); Paulo S. Grassi, *Letter of Credit Transactions: The Bank's Position in Determining Documentary Compliance: A Comparative Evaluation Under U.S., Swiss and German Law*, 7 *PAGE INT'L L. REV.* 81, 118–21 (1995) (describing different standards of strict compliance under domestic letter of credit law). This article, however, is concerned solely with domestic payment systems rules. For a cross-country comparison of the different frequencies of use of paper instruments and electronic payments, see David B. Humphrey, Lawrence B. Pulley & Jukka M. Vesala, *Cash, Paper, and Electronic Payments: A Cross-Country Analysis*, 28 *J. MONEY, CREDIT & BANKING* 914 (1996).

2. Under the Truth-In-Lending Act, an “unauthorized use” of a credit card means use by a person “other than the cardholder who does not have actual, implied, or apparent authority for such use.” 15 U.S.C. § 1602(o) (2000). Under the Electronic Fund Transfer Act, however, an “unauthorized electronic fund transfer” means a transfer from a consumer’s account initiated by a

appear to be exacerbated by the current spate of new payment mechanisms, combined with increasing international transactions that entail some form of payment. Together, these concerns underlie the push for uniformity among payment systems, both domestically and internationally.

But diversity in payment systems produces some unsung benefits. The form in which payment is made is part of the transaction that calls for payment. It therefore is an express or implied term that allocates risks within that transaction, no different in this respect from the transaction's other terms. Payment systems themselves entail multiple risks, each of which is likely to be priced into the transaction—at least in transactions involving sophisticated parties or thick markets. First, payments rules allocate risks of fraud and error in the underlying transaction. A buyer of goods, for instance, might prefer paying with a check that is susceptible to a stop-payment order and that therefore affords the buyer a longer period for inspection for nonconformities than payment by debit card. Second, payments rules allocate risks of fraud or error with respect to the payment mechanism itself. For example, any payment mechanism is vulnerable to the risk that an unauthorized person will demand payment from an obligor. Different parties, or different classes of parties, may have different preferences about the best way to allocate these risks, either because they have different levels of risk preference or different capacities for risk reduction through means other than payment systems. In addition, different transactional structures may warrant different treatment of each of these risks, perhaps because different parties are in a superior position to avoid the risks that could materialize with respect to payment in different transactions. For instance, the long-distance sale of goods may warrant default payment rules that differ from payment rules for services performed on a face-to-face basis. Third, different payment systems entail different allocations of credit risk. Checks shift to payee-sellers (at least initially) the risk that the drawer-buyer is insolvent. Debit and credit cards avoid that risk to the extent that authorization for the transaction confirms a simultaneous deduction from the user's bank account or imposes a payment obligation on the card issuer.

person other than the consumer without actual authority to initiate such transfer." 15 U.S.C. § 1693a(11). It is unclear why a person with implied or apparent authority would be included in the first definition, but excluded from the second. See James Steven Rogers, *The Basic Principle of Loss Allocation for Unauthorized Checks*, 39 WAKE FOREST L. REV. 453, 474 n.66 (2004).

In order to take advantage of these different risk allocations, parties might prefer a menu that consists of a limited number (but greater than one) of payments options, each accompanied by its own default rules. Faced with such a menu, parties would have the opportunity to make a low-cost selection of a payment device that allocates risks in a manner consistent with their particular transaction. One might respond that uniform rules are still appropriate, as long as payment rules are only defaults, because individual parties could bargain for highly tailored rules that best suit their own transaction. That response would make sense if a significant majority of parties desired the single uniform rule, so that bargaining around the default involved relatively few parties and thus minimal costs. But it may be that no such majoritarian default exists. Instead, each of a variety of different rules may command acceptance from a substantial minority of actors, depending on the nature of the transaction and the relative capacity of the parties to reduce the risks inherent in both the underlying transaction and in the payment system. For instance, the buyer in one transaction may be relatively capable of monitoring seller behavior, and thus be willing to release funds with a limited right to reverse payment, while a buyer in another transaction would prefer a payment mechanism that reflects the capacity of a third-party payer to monitor the seller, and a buyer in a third transaction may be sufficiently skeptical of seller performance that she desires to retain the right to countermand any payment order. If the market for payments was segmented so that parties could select among various payment systems, each of which came with well-understood, overlapping, but non-identical default rules, then permitting parties to select from a menu of devices may be superior to the choice between uniform default rules and a fully bargained risk allocation. Under these circumstances, the parties in each case would presumably prefer to select a pre-packaged, state-supplied payment system accompanied by rules that approximated the parties' desired risk allocation, rather than to bargain for that same risk allocation where it deviated from a uniform rule.

This is not to say that standardization is never warranted. It is only to say that uniformity must be argued for rule by rule. It may, for instance, be possible to identify a set of transactions or transacting parties for whom the benefits of uniformity clearly dominate, perhaps because the costs of learning the intricacies of different payment rules are not worth incurring. For those transactions, it would be preferable to have a set of default rules that cut across payment systems. For instance, if consumers as a group are systematically likely to be confused

by a multiplicity of risk allocation rules that would otherwise be optimal, it might be desirable to create uniform default rules for payment systems that consumers tend to use, while allowing more variation among payment systems that are more prevalent in business transactions. But even in the case of consumers, the potential for confusion generated by multiple payment rules must be weighed against benefits that would be generated by diversity in payment systems rules. Once one considers those benefits, it is plausible that education to increase consumer awareness would create more welfare than making legal rules more uniform.

In this Article, we explore the parameters of the optimal standardization of payments law. We do not attempt to determine the optimal level of specificity for payment rules. For instance, one could imagine that a user of a payment system, such as a credit card, could be given a variety of options concerning matters such as fraud risk and payment risk that would be negotiated or selected with every use of the card. Such “within-system” menus would provide more detailed pre-set options than “among-system” menus that exist when each system incorporates a single set of default rules, but would also avoid the need to negotiate a complete set of risk allocations from scratch with every use of the payment system. Rather than arbitrate the appropriate degree of specificity, our objective in this article is to consider the characteristics of different payment systems that a designer of optimal rules would want to consider in defining the appropriate scope of uniformity.

Underlying our argument is a presumption that commercial law, including the law of payment systems, should do for parties what they would otherwise do for themselves.<sup>3</sup> Achieving this objective reduces

3. An implication of our thesis is that payment system rules should include state-supplied default rules that are diverse across payment systems. An argument against state-supplied default rules is that they are not needed. Parties instead can supply the terms of their payment obligations and rights at low cost, making the setting of default rules unnecessary. Alternatively, trade groups or market participants, such as automated clearing house associations or card system providers, can set default rules. In both cases state-supplied default rules, whether uniform or diverse, are unnecessary. We reject this “irrelevance” argument. Even if the cost of providing terms that default rules otherwise provide is low, the cost is positive. Aggregated over transactions, transaction costs are high. Default rules avoid this cost. The possibility that private actors might supply default terms does not make state-supplied terms unimportant. Market structure might prevent trade groups or participants, for a significant time, from settling on a set of default terms. The delay in adopting shared standards of container dimensions in the container transport industry is an example; see MARC LEVINSON, *THE BOX* 127–49 (2006). Where market actors prefer the defaults set by the state, they are saved the cost of providing their own defaults. Modest transaction cost savings and the possibility that defaults will be provided privately therefore do not show that state-supplied defaults are unnecessary. There is a stronger case for limiting de-

transactions costs in commercial interactions. Implicit in that thesis is a belief that the absence of a majoritarian default does not entail the desirability of a single rule across payment systems. Just as the different optimal default rules for warranties for finance leases, sales of goods and technology licenses reflect features of those transactions, the optimal rules for payment systems probably vary according to different transactions and transactors. There is no more reason to believe that a single set of rules is optimal for all payment devices than there is to believe that a single set of terms is optimal for every sort of transaction that generates a payment obligation. Indeed, creating uniform legal rules may undermine the realization of uniform objectives that the legal rules purport to serve. For instance, we claim below that a general objective for allocating the risk of fraud is to place fraud losses on the party in the best position to avoid them. But it is not clear that the same party occupies that position across payment systems. Thus, a legal rule that uniformly placed the risk of loss on the same party across payment systems would fail to serve the objective that presumably motivates each payment system.

Notwithstanding our claim that legal defaults should reflect parties' preferences, we do not claim that payment system users systematically select among systems based on legal rules. Many users will be unaware of the rules that accompany their selections. Consumers in particular are likely to be ignorant of the risk allocations embodied in legal defaults. Even those who have some awareness of legal rules may choose among payment systems based on convenience, rather than risk allocations. A customer who has access to both checks and a debit card may use the latter, even if she believes that the law of checks is more consumer friendly, because swiping a card provides an easier, quicker form of payment in a long checkout line than writing a check. But the fact that users do not select their systems based on legal rules does not mean that those rules are irrelevant. Users presumably would still prefer that the rules reflect the hypothetical risk allocation that relatively informed parties would have struck, since that bargain is likely to have price or other *ex ante* effects. Certainly in a situation, such as payment systems, where there is likely to be asymmetric information (since payment system providers are likely to be aware of the legal rules even if system users are not) creating defaults that re-

fault rules to situations that describe only a few possible states of the world, that are relatively simple in form, and that are efficient for a wide variety of contract parties. See Alan Schwartz & Robert E. Scott, *Contract Theory and the Limits of Contract Law*, 113 *YALE L.J.* 541, 598 (2003).

flect a hypothetical bargain would appear useful in order to avoid advantage-taking.

The fact that users make selections among payment systems on bases other than legal rules, however, may dilute the arguments about the desirability of uniformity in some contexts. For instance, we engage the argument that uniformity in legal rules is necessary to avoid distortion in the use of payment systems. But if users do not consider legal rules in choosing among payment systems, then legal rules are unlikely to cause any distortion. They will only have *ex post* distributive effects. Even with respect to distortion, however, the proper level of uniformity may be a relevant datum. First, even if many users are ignorant of or indifferent to the legal rule, other users may be attentive, and distortion arguments are at least relevant to them. Second, the *ex post* distributive effects may themselves be important, especially with respect to consumers, who may be the least knowledgeable of the legal implications of their payment system choices.

In what follows, we elaborate on these observations and apply our thesis in the context of various payment system rules. The Article is in three parts. Part I briefly describes the diversity of rules across non-cash payment systems. Part II critically evaluates several arguments in the literature recommending uniformity in payment systems law. It concludes that the proposals overestimate the reduction in information costs resulting from standardization of rules and underestimate or ignore the benefits of a choice among instruments with different rules. Part III makes the case that the optimal standardization of payment system rules allows diverse rules among payment systems. It applies Part II's argument to rules on unauthorized payment, reversibility rules for credit and debit cards, and preclusion rules for checks and wire transfers. In doing so, Part III argues that current law in these areas does not reflect an optimal standardization in rules across payment systems. Part III also contains a qualified defense of the distinction in some payment systems law between consumers and non-consumers of payment instruments.

#### I. DIVERSITY IN PAYMENT SYSTEM RULES

The legal regime that governs any payment system typically contains rules that allocate three different risks between the payment system provider (typically the bank that issues a card or letter of credit or on which a check is drawn) and its user (the cardholder or drawer or payee of the check or applicant on a letter of credit): unauthorized

payment, erroneous payment, and reversibility of payment instructions. These rules vary to a greater or much lesser extent across payment devices.<sup>4</sup> Rules governing unauthorized and erroneous payment bear more similarity among payment systems than rules governing reversibility. Even where rules governing unauthorized and erroneous payment are generally similar, however, exceptions, liability limits, defenses, and burdens of proof vary. Case law in some instances also creates different rules from formally similar statutory rules, although in other cases, formal differences are diluted by judicial decisions.<sup>5</sup> Differences among the respective rules are in the details. More generally, payment systems law treats some of these rules as default or mandatory rules depending on the particular payment system they control.<sup>6</sup> The sections below briefly describe the contours of the three rules across principal non-cash payment systems.

#### A. *Unauthorized Payment*

The law of most non-cash payment systems places all or part of the risk of unauthorized payment on the system provider. However, the extent of a payment system provider's liability varies across systems. Where payment is by check, unauthorized payment typically means either that the drawer's signature or the payee's signature has been forged. The party whose signature has been forged is generally not liable for payment made under these conditions.

Similarly, an issuer of letter of credit is not entitled to reimbursement from its applicant when it honors a draw that does not comply with the terms of the credit.<sup>7</sup> The consumer credit card holder is not legally liable for losses in excess of \$50 arising from an unauthorized

4. See Ronald J. Mann, *Making Sense of Payments Policy in the Information Age*, 93 GEO. L.J. 633 (2005). For general descriptions of payments law finding more uniformity in rules than the description below, see Rogers, *supra* note 2, at 453.

5. For instance, the definition of an unauthorized use of a credit card, for which a cardholder has very limited liability, does not include a requirement that the cardholder exercise ordinary care in reviewing statements. That requirement does apply to limit the liability of a drawer with respect to unauthorized checks. Nevertheless, some courts have determined that a cardholder's failure to review statements constitutes a grant of apparent authority, which will transform an unauthorized use into an authorized one for which the cardholder is responsible. See *Borg v. Chase Manhattan Bank USA, N.A.*, 247 F. App'x 627 (6th Cir. 2007); *Carrier v. Citibank (S.D.)*, N.A., 180 F. App'x 296, 297 (2d Cir. 2006); *Minskoff v. Am. Express Travel Related Serv. Co.*, 98 F.3d 703, 709 (2d Cir. 1996).

6. Cf. U.C.C. §§ 4-103(a), 4A-501(a), 5-103(c) (2005) (checks, wire transfers, and letters of credit, respectively); 15 U.S.C. § 1643(d) (consumer credit cards); 15 U.S.C. § 1693g(e) (consumer electronic funds transfers).

7. U.C.C. § 5-108(i).

use of its credit card.<sup>8</sup> The consumer who utilizes an access device to initiate an electronic fund transfer is liable for losses that range from \$50 to the entire loss arising from unauthorized use of the device, depending on whether the lost card is timely reported.<sup>9</sup> Where the unauthorized payment is by wholesale wire transfer, the customer identified as the sender is not liable for the loss unless the bank authenticated the payment order using a commercially reasonable security procedure established with the customer; even if the bank satisfies that condition, the customer will bear no liability if it can prove that the order was issued by someone other than an agent who was entrusted by the customer to act with respect to payment orders or by a person who did not access the customer's transmitting facilities.<sup>10</sup>

User negligence or inattention plays varied roles with respect to unauthorized payments. It plays a prominent role in reallocating losses in check systems. The initial allocation to the payment system provider can be reversed if the user failed to take advantage of a superior position to avoid the loss—a phrase that is not coterminous with negligence, but is at least suggestive of its presence.<sup>11</sup> User failure to review bank statements and notify the bank of forgeries will preclude that party from asserting subsequent forgeries by the same wrongdoer.<sup>12</sup> Although check system providers can also shift losses back to users under some circumstances that do not expressly require individualized investigations into negligence, those circumstances involve situations where the user arguably has been presumptively negligent, such as by delivering a check to an imposter whose true identity the user could have readily determined.<sup>13</sup> Thus, even where user negligence is not an explicit factor in allocating losses, it may be implicit in the legal loss allocation. A common scenario, in which an employer fails to monitor a

8. 15 U.S.C. § 1643(a)(1). The norms of the credit card industry have reduced this liability to zero under most circumstances. *See, e.g.,* Mastercard, Zero Liability, <http://www.mastercard.com/us/personal/en/cardholderservices/zzeroliability.html> (last visited Mar. 26, 2008), Visa, Zero Liability, [http://usa.visa.com/personal/security/visa\\_security\\_program/zero\\_liability.html](http://usa.visa.com/personal/security/visa_security_program/zero_liability.html) (last visited Mar. 26, 2008). *Cf.* 15 U.S.C. § 1645 (business which provides credit cards to its employees may agree not to be subject to § 1643's liability limits).

9. 15 U.S.C. § 1693g(a). *See* Clayton P. Gillette, *Rules, Standards, and Precautions in Payment Systems*, 82 VA. L. REV. 181, 183 (1996).

10. U.C.C. §§ 4A-202, 4A-203.

11. *Id.* §§ 3-404, 3-405, 3-406(a), 4-401(a). The drawer may have been negligent in the situations where it is in a superior position to avoid the loss and failed to take precautions, but the drawer will bear the loss in such situations even if there is no negligence.

12. *Id.* § 4-406(d).

13. *Id.* § 3-404(a).



disloyal employee who had responsibility with respect to checks, leads to employer liability for forgeries even if the employer was non-negligent in its supervision.<sup>14</sup> But the cases suggest that negligence is the norm in such cases, at least insofar as the employee's defalcations go undetected for a significant period of time.<sup>15</sup> User negligence combined with a bank's own failure to exercise ordinary care in these situations will cause losses to be divided according to a comparative contribution standard.<sup>16</sup>

Losses in other payment systems, however, are allocated in accordance with principles of authority that arguably coincide less with principles of negligence. As noted above, the loss from an unauthorized wholesale payment order is allocated in accordance with principles of agency law and compliance with security procedures rather than by any reliance on negligence principles.<sup>17</sup> A bank that authenticates a payment order pursuant to a reasonable security procedure to which the bank and the customer agreed will be able to impose the loss from an unauthorized payment order, even if the customer exercised due care in protecting access to its transmission facilities. Liability can be avoided only if the customer can prove that the wrongdoer was not a person who acted for the customer with respect to payment orders or the security procedure, or who accessed the transmitting facilities of the customer.<sup>18</sup>

Nor does negligence play any explicit role in the allocation of losses that emerge from consumer use of credit cards and electronic fund transfers. Consumer responsibility (above the \$50 limitation) in those cases depends solely on whether use of the card was "authorized." That concept, in turn, is defined in terms of agency law, not in terms of negligence. A consumer who writes his personal identification number on the back of his debit card and leaves the card conspicuously on his office desk will not be responsible beyond the statutory limit if a thief steals the card and uses it to make purchases after discovering the PIN number on the back.<sup>19</sup> Some cases that involve repeated fraudulent use controversially equate failure to review monthly state-

14. *Id.* § 3-405.

15. *See, e.g.,* *Rodrigue v. Olin Employees Credit Union*, 406 F.3d 434, 449 (7th Cir. 2005); *Panhandle Packing & Gasket, Inc. v. First United Bank*, No. 07-05-0426-CV, 2007 WL 2522695, at \*2 (Tex. App. Sept. 6, 2007).

16. U.C.C. §§ 3-404(d), 3-406(b), 4-406(e).

17. *Id.* § 4A-202(a)-(b).

18. *Id.* § 4A-203(a)(2).

19. *See* 12 C.F.R. pt. 205, supp. I, § 205.6, cmt. 6(b), note 2 (2007).

ments with grants of apparent authority to use a card.<sup>20</sup> Those same cases imply that failure to review is indicative of user negligence. But even those cases do not explicitly embrace negligence as the standard of loss allocation.

Uniformity is further undermined by different definitions of “unauthorized” in the Truth-in-Lending Act, which governs credit cards, and the Electronic Fund Transfer Act, which governs debit and ATM cards. The former defines the term to include use of a credit card by a person other than the cardholder who does not have “actual, implied, or apparent authority.”<sup>21</sup> The latter, however, defines an “unauthorized electronic fund transfer” as a transfer initiated by a person other than the consumer “without actual authority to initiate such transfer.”<sup>22</sup> Taken literally, this distinction leads to the ostensibly anomalous result that a holder of a card that could be used for either a debit or credit transaction would be responsible if she granted apparent authority to a third party who fortuitously hit the “credit” button while initiating the transaction, but not if that same person hit the “debit” button.<sup>23</sup>

Diversity also extends into the scope of liability for unauthorized payment. With respect to checks, a drawee that is liable for an unauthorized payment is typically responsible for the amount of the check, but an unauthorized payment could lead to failure to honor authorized payments with more serious consequences for the bank.<sup>24</sup> The law governing wholesale payment orders, on the other hand, makes no provision for consequential damages in the event that an unauthorized payment order has been executed. The bank must reimburse the customer only in the amount of the debit, plus interest, upon timely notice of objection by the customer.<sup>25</sup> The issuer of a letter of credit that honors an unauthorized draw on the credit is not liable to its applicant for

20. *See, e.g.*, *Borg v. Chase Manhattan Bank USA, N.A.*, 247 F. App'x 627 (6th Cir. 2007); *Carrier v. Citibank (S.D.), N.A.*, 180 F. App'x 296, 297 (2d Cir. 2006); *Minskoff v. Am. Express Travel Related Serv. Co.*, 98 F.3d 703, 709 (2d Cir. 1996).

21. 15 U.S.C. § 1602(o) (2000).

22. 15 U.S.C. § 1693a(11).

23. For discussion of “smart cards” that can be used for either debit or credit functions, see Arnold S. Rosenberg, *Better than Cash? Global Proliferation of Payment Cards and Consumer Protection Policy*, 44 COLUM. J. TRANSNAT'L L. 520, 529 (2006).

24. *Cf.* U.C.C. § 4-402(b) (payor bank liable to its customer for damages “proximately caused” by wrongful dishonor of item). For description of the divergence in courts’ allowance of recoverable damages under section 4-402(b), see CLAYTON P. GILLETTE, ROBERT E. SCOTT & ALAN SCHWARTZ, *PAYMENT SYSTEMS AND CREDIT INSTRUMENTS* 517–32 (2d ed. 2007); WILLIAM D. WARREN & STEVEN D. WALT, *PAYMENTS AND CREDITS* 349–51 (7th ed. 2007).

25. *See* U.C.C. §§ 4A-204, 4A-402, 4A-505 & cmt.

consequential damages resulting from the draw.<sup>26</sup> The issuer remains liable for incidental expenses incurred by the applicant in connection with unauthorized honor. Given the different allocations of liability and limitations on recovery for unauthorized payment across payment systems, “the risk is on the payment provider” misstates the law.

### B. Payment Error

Rules governing errors in payment are more uniform across payment systems. As between the owner of the account erroneously charged and the payment system provider, the latter generally bears risks of errors in the transfer of payment.<sup>27</sup> Although no statutory provision expressly allocates errors in the payment of checks, the working assumption, which permits drawee banks to debit customers’ accounts only in respect of checks that are “properly payable,” appears to allocate payment error to the payment provider. The assignment of liability arising from the misencoding of checks demonstrates this implicit allocation. The payor bank honoring an over-encoded check is liable to the drawer for the over-encoded amount debited from its account.<sup>28</sup> The person over-encoding the check in turn is liable to the payor bank.<sup>29</sup> Both the payor bank and the encoding person’s respective liabilities presuppose that the drawer does not bear the risk of errors in payment. A letter of credit issuer is not entitled to reimbursement from its applicant if it honors a draw in violation of the terms of the reimbursement agreement with the applicant.<sup>30</sup> For its part, the receiving bank is liable for errors in execution of a payment order, but not for consequential damages resulting from the erroneous execution.<sup>31</sup> A credit or debit card issuer is liable to a consumer cardholder for errors in charges or debits to the cardholder’s account.<sup>32</sup>

26. *Id.* § 5-111(b) (liability for wrongful dishonor or honor of a credit).

27. The payment provider is typically allowed to recover the mistaken payment from the party unjustly enriched by it, though a recipient of funds who received them in good faith and for value, or who changed position in reliance of the payment, may resist claims for recovery. *See, e.g., id.* §§ 3-418, 4A-303(a).

28. *See id.* §§ 4-209 cmt. 2, 4-402(b).

29. *Id.* § 4-209(a).

30. *Id.* § 5-111(i). The statement in the text ignores the issue raised by draws on credits containing typographical errors in documents inconsistent with the terms of the credit. It assumes that such errors render the documentary presentation non-complying under the controlling standard of documentary compliance. *See, e.g., Beyene v. Irving Trust Co.*, 762 F.2d 4, 6 (2d Cir. 1985); *Hanil Bank v. PT. Bank Negara Indonesia*, 41 UCC Rep. Serv. 2d 618, 622–23 (S.D.N.Y. 2000).

31. U.C.C. §§ 4A-303, 4A-402(c), 4A-305(b).

32. 15 U.S.C. § 1693f(a) (2000) (debit card); 15 U.S.C. § 1666(a)–(b) (credit card).

### C. Reversibility of Payment Instruction

Reversibility of a payment instruction allocates the risk of dissatisfaction with the underlying transaction rather than with a fraudulent payment transaction. A payment system user may discover that goods or services were not as represented and thus seek to countermand an instruction previously given to the payment service provider to pay the seller of the goods or services. The right of the payment system user to countermand that instruction, however, varies significantly across payment systems. Some payment system rules allow the payment system user to countermand a payment instruction when there is a dispute over performance of the underlying transaction; others do not. Those that do not are consistent with the rules that apply in a cash transaction. Typically, a buyer who pays with cash will bear the burden of proving the defective nature of the transaction and will be unable to recover the payment until that burden is met.<sup>33</sup>

Non-cash payment systems deviate from the “cash” rule in varying degrees. For checks, the drawer has no right to have its deposit account recredited after the payor bank has made final payment. Payment is complete when the check is paid in cash or the payor bank has become obligated to finalize a settlement for the check.<sup>34</sup> Until that time, however, the drawer may issue a stop payment order that obligates the drawee to dishonor a check, but only if that check has been drawn on the account of the person issuing the stop payment order.<sup>35</sup> A seller of goods or services may avoid reversibility by demanding an instrument that cannot be countermanded because of buyer dissatisfaction, such as a cashier’s check or a teller’s check.<sup>36</sup> Thus, even within the single payments system of checks, some diversity is permitted to respond to different preferences for allocating risks related to the underlying transaction.

The right of a consumer credit card user to countermand an instruction for the card issuer to pay the seller is even more complicated. The right of reversibility does not hinge on whether the card issuer has paid the seller. Rather, it depends on the nature of the underlying dispute, the location of the transaction, and the extent to which the card user has notified the card issuer of the dispute. If the dispute involves

33. See Paul M. Shupack, *Cashier’s Checks, Certified Checks, and True Cash Equivalence*, 6 *CARD. L. REV.* 467, 467 (1985).

34. U.C.C. § 4-215.

35. *Id.* § 4-402.

36. See *id.* § 3-411.

the quality of the seller's performance, the card user may assert against the card issuer any defense against payment that the card user had against the merchant. At least, that is the case if the card user has made a good faith attempt to resolve the issue with the seller, the amount of the transaction exceeds \$50, and the place where the initial transaction occurred was in the same state as the location of the cardholder or within 100 miles of that location.<sup>37</sup>

The rule is arguably different where the alleged defect in the underlying transaction involves non-delivery rather than delivery of defective goods or services. Under those circumstances, the card user arguably can treat any reference to the defective transaction on a statement from the card issuer as a billing error.<sup>38</sup> Countermand of the transaction would not be subject to the geographical and other limitations that apply to transactions in which there has been faulty performance, but not nonperformance. Instead, the card user who gives due notice to the card issuer<sup>39</sup> could impose on the card issuer a duty to investigate the transaction and withhold payment of the charge reflected on the statement.

The consumer debit card user has no right similar to that of the credit card user who desires to assert defenses against the card issuer. The debit card user has a right to have her account recredited only if the account contains an error.<sup>40</sup> The relevant errors, however, are defined more narrowly than "billing errors" for credit card purposes. A qualitatively defective transaction, including non-delivery, arguably falls outside the statutory scope of errors that obligate the debit card issuer to recredit the consumer's account.<sup>41</sup>

The letter of credit is typically viewed as a mechanism for shifting to the buyer the risk of dissatisfaction with the quality of goods. Thus, the letter of credit issuer is obligated to make payment to the beneficiary notwithstanding any objection from the applicant. The applicant's recourse against the beneficiary in connection with performance of the underlying transaction is against the beneficiary, not the issuer.<sup>42</sup> The applicant has a basis for countermanding the instruction to pay only if the documents that the beneficiary presents fail to comply with the terms of the credit, or if the applicant can satisfy the high standard of

37. 15 U.S.C. § 1666i(a).

38. *See id.* § 1666(b)(3); Mann, *supra* note 4, at 648-49.

39. *See* 15 U.S.C. § 1666(a).

40. 15 U.S.C. § 1693f.

41. *Id.* § 1693f(f).

42. *See* U.C.C. § 5-110(a)(2).

demonstrating that honor would facilitate a material fraud by the beneficiary.<sup>43</sup>

For a wire transfer, a sender's cancellation or amendment of a payment order is effective if the receiving bank receives it when it has a reasonable opportunity to act before executing the order.<sup>44</sup> Acceptance of the order by a receiving bank obliges the sender to pay the amount of the order.<sup>45</sup> After acceptance, cancellation may still be effective if the receiving bank agrees or a funds-transfer system rule permits cancellation.<sup>46</sup> Cancellation of an accepted payment order is permitted in very limited circumstances.<sup>47</sup> Automated clearing house rules for non-consumer credit and debit transfers provide for the same result.<sup>48</sup>

This brief discussion reveals the significant divergence among payment systems with respect to a variety of risks that affect both the mechanism of payment and the underlying transaction. It might be thought to provide significant fodder for the argument that payment systems are irrationally diverse and that the differences in risk allocations reflect a combination of path dependence and historical contingency, rather than any well-considered effort to design an optimal allocation of payment-related risks. In the next section we outline and critique the general argument for eliminating these significant differences. We ultimately contend that these arguments are less persuasive than one might initially believe. That raises the possibility, which we pursue in Part III, that substantial diversity in payment systems rules, though not necessarily the current level of diversity, is actually optimal.

## II. ARGUMENTS FOR UNIFORMITY

Diversity in rules across payments law is desirable only if the associated benefits offset the costs of learning and confusion that are minimized by uniformity. Much academic literature and many law reform efforts assume without argument that uniformity is superior. But the assumption that uniformity is desirable is not self-evident. Because

43. *Id.* § 5-109(a).

44. *Id.* § 4A-211(b).

45. *Id.* § 4A-402(c).

46. *Id.* § 4A-211(c).

47. *Id.* § 4A-211(c)(1)–(2).

48. See NAT'L AUTOMATED CLEARING HOUSE ASS'N, 2006 ACH RULES: CORPORATE EDITION § 8.5, at OR 23 (2006); *cf. id.* § 8.4, at OR 23 (providing a three-day rule for stop payments for consumer accounts).

payment terms are part of transactions calling for payment, optimal rules for payment also are part of the optimal rules governing the transaction. The optimal set of terms minimizes the sum of the costs of planning, performing, and enforcing the transaction. If a single set of rules were optimal for all or most transactions, a presumption favoring uniformity in rules would be defensible. However, it would be miraculous if the same rules (terms) were optimal for all or most transactions, without regard to their subject matter, the characteristics of the transactors, and transactors' relationships to each other.<sup>49</sup> An implied warranty of merchantability may be an optimal implied term for most sales of goods contracts with a merchant seller, since the merchant seller, as a repeat player with respect to the goods, is likely to have superior information about defect rates of the goods he or she is selling. The term is unlikely to be optimal for typical sales contracts where the seller is a non-merchant, since non-merchants will not necessarily have better information about the goods than the buyer. Likewise, non-cash forms of payment can be selected in some cases because they place risks of safety or the delay in final payment on a seller, who may be better positioned than buyers to take those risks.<sup>50</sup> Both examples show that a presumption favoring uniformity in rules is not axiomatic. Proposals recommending that the same rules should apply across non-cash payment systems therefore must be argued for, not assumed.

Of the different senses of "uniformity," only uniformity in substantive rules is at issue. Uniformity in the source of payment system rules is not. Rules regulating forms of payment may have a single or multiple sources, such as federal or state law or a rule-producing organization. Within federal or state law, rules also may be better located in a single statute or regulation.<sup>51</sup> The preferable source of payments law depends in part on institutional considerations about the production of legal rules. A single source of law reduces the cost of organizing dispersed interests to initiate or alter rules. At the same time, a single source of law also makes it easier for a cohesive interest group to de-

49. This is the lesson of the law and economics literature on the efficient choice of contract remedy, where ex ante and ex post effects make it unlikely that restitution, reliance, or expectation recoveries are optimal.

50. See generally Daniel D. Garcia-Swartz, Robert W. Hahn & Anne Layne-Farrar, *The Move Toward a Cashless Society: A Closer Look at Payment Instruments Economics*, 5 REV. NETWORK ECON. 175 (2006), [http://www.rnejournal.com/articles/garcia\\_swartz\\_1\\_RNE\\_june\\_2006.pdf](http://www.rnejournal.com/articles/garcia_swartz_1_RNE_june_2006.pdf); Humphrey et al., *supra* note 1.

51. See, e.g., Fred H. Miller, *A Report on the New Payments Code*, 39 BUS. LAW. 1215, 1215-16 (1984) (describing reasons offered by the "348 Committee's" 1978 report recommending proposed Uniform New Payment Code); see also *infra* note 54.

termine the output of the lawmaking body by dominating its lawmaking process.<sup>52</sup> Multiple sources of law, by making possible the production of diverse rules governing the same issue, may make it more likely that particular rules that satisfy social interests will be enacted. Institutional concerns about a single or multiple sources of law are different from concerns about the desirable degree of uniformity in the substance of rules of payments law. This Part considers and rejects some traditional arguments for uniformity in substantive rules.

#### A. *Article 9 as Precedent*

The enactment of uniform rules governing other subjects might suggest that similar uniformity is desirable for payment systems. Article 9 of the Uniform Commercial Code is an example of a widely adopted uniform set of rules with very few non-uniform amendments made by enacting states. Prior to Article 9's enactment, chattel mortgage acts, conditional sales acts, and trust receipts acts sometimes imposed different requirements for notice and filing, regulation of after-acquired collateral, and rules concerning the debtor's continued control of collateral or proceeds. Article 9 replaced these different statutory and decisional rules with a single statute containing the same basic rules applicable to all security interests in personal property.<sup>53</sup> Judged by the extent and speed at which both Article 9 and its revision have been enacted at the state level, Article 9's provision of a uniform law for secured transactions is a success. Article 9 therefore might suggest that a uniform law of payment systems is desirable. Indeed, the drafters of the proposed 1983 Uniform New Payments Code regarded Article 9 as a favorable analogy.<sup>54</sup>

Even if Article 9 supplies a single set of rules to govern similar transactions, however, it is not a precedent for a uniform law of payment systems. The factors that might justify the same basic rules for all secured transactions in personal property are not present with different forms of payment. Simply put, Article 9 governs transactions involving creditors within a fairly predictable range of abilities to

52. See Alan Schwartz & Robert E. Scott, *The Political Economy of Private Legislatures*, 143 U. PA. L. REV. 595, 643-44 (1995) (applied to the ALI and NCCUSL process of creating Articles 3 and 4 of the U.C.C.).

53. See U.C.C. § 9-102(2) (2000) (prerevision U.C.C., stating: "This Article applies to security interests created by contract including pledge, assignment, chattel mortgage, chattel trust . . . conditional sale, trust receipt . . .").

54. HALL S. SCOTT, *NEW PAYMENT SYSTEMS: A REPORT TO THE 3-4-8 COMMITTEE OF THE PERMANENT EDITORIAL BOARD FOR THE UNIFORM COMMERCIAL CODE* 1, 38-40 (1978).



provide and make use of information, and to monitor particular assets of the debtor. For instance, monitoring capacity may vary among types of collateral, but those who are well positioned to monitor collateral in one form of transaction are likely to be similarly well positioned with respect to the same form of collateral used in another type of secured transaction.

Article 9's rules, if justified, optimally reduce the size of the debtor's total debt bill. Because a debtor's debt bill reflects monitoring costs creditors incur in connection with their loans, the debtor will issue secured debt so as to minimize the sum of associated monitoring costs. Consistent with this rationale, both Article 9's basic first-to-file-or-perfect rule and its exceptions allocate the debtor's assets to the superior monitor among secured creditors.<sup>55</sup> From this point of view, the fact that a secured transaction involves inventory or accounts or any other sort of tangible or intangible collateral is irrelevant. Whatever the collateral, rules governing security interests in it optimally reduce the related monitoring costs. For the same reason, the same rules should apply to the transaction whether it takes the form of a chattel mortgage, conditional sale, or delivery of trust receipts.

Article 9's rules rest on two assumptions about the behavior of secured creditors: (1) that they use Article 9's notice filing system to discover information about existing or potential security interests, and (2) that the debtor and its secured creditors partition the debtor's assets among secured creditors according to the creditors' comparative advantage at monitoring them. If secured creditors don't use information from the notice filing system, their monitoring won't reliably reflect that information. And if creditors differ markedly in their monitoring abilities, then Article 9's exceptions to its first-to-file-or-perfect rule might not accurately track these abilities among creditors. In a spectrum of potential creditors, Article 9's rules best reflect the characteristics of banks and finance companies, not consumer creditors, sole proprietors, or small businesses.<sup>56</sup> These creditors most re-

55. See, e.g., U.C.C. §§ 2-322(a)(1), 9-324(a)-(b), 9-330(a)-(b), 9-332 (2005) (first-to-file-or-perfect priority, purchase money superpriority, priority of certain chattel paper purchasers, and priority of transferees of funds or money, respectively). Cf. REINIER KRAAKMAN ET AL., *THE ANATOMY OF CORPORATE LAW* 8-9 (2004); George G. Triantis, *Organizations as Internal Capital Markets: The Legal Boundaries of Firms, Collateral, and Trusts in Commercial and Charitable Enterprises*, 117 HARV. L. REV. 1102, 1138-39 (2004).

56. See, e.g., U.C.C. §§ 9-104(a), 9-327, 9-332, 9-340 (favoring banks); see also *id.* § 9-330 (finance companies). For the role of banks and finance companies in the early revision process of Article 9, see Robert E. Scott, *The Politics of Article 9*, 80 VA. L. REV. 1783, 1822-23 (1994); Schwartz & Scott, *supra* note 52, at 638-39.

liably satisfy the implicit behavioral assumptions that justify a single set of rules applicable to all secured transactions in personal property. Where the characteristics of consumer debtors are likely diverse, revised Article 9 either excludes from Article 9's scope a range of consumer protection rules or adopts special provisions applicable to consumers.<sup>57</sup> The treatment leaves its remaining rules uniform, but also indicates that the drafters were willing to deviate from uniformity where the rules applicable to some transactions did not serve the overall objectives of the Article with respect to other transactions.

In contrast, the range of transactions and characteristics of transactors using different forms of payment is much less uniform. Some payment systems typically involve two parties, some involve three parties, some—but not all—implicate multiple repeat players, some—but not all—involve sophisticated risk-reducing technology that is systematically available to a person ordering payment, some involve other similarly sophisticated risk-reducing technology that is systematically available to a person making payment. The cost to payment system providers in detecting payment error or controlling against unauthorized payment, for example, may sometimes be less than and sometimes greater than the cost to alternative parties to the transaction. Presumably, the parties to any payment transaction would prefer the payment system provider to bear the relevant risks in the former case, but not in the latter, since placing the risks on the parties best positioned to avoid them minimizes the costs of using the system for all parties. Competition among payment systems would presumably allow for sorting among these different preferences. Moreover, the characteristics and preferences of payment system users are more diverse than those of creditors who take advantage of the various applications of Article 9. Payment system users range in their sophistication about the rules and consequences of the form of payment they use; in addition, this sophistication varies between consumers, sole proprietors, and small businesses. The ability to avoid or reduce a relevant payment risk also may vary among payment system users using different payment systems. Further, users of different forms of payment may have different preferences as to convenience, security of payment, access to a line of credit, and the float of funds. Equally important may be the episodic character of the form of payment used. Unlike the issuance

57. See, e.g., U.C.C. §§ 9-103(h), 9-626(b) (making relevant provision inapplicable to consumer-goods transactions); see also *id.* § 9-108(e)(2) (special rule for collateral descriptions in a consumer transaction).

of secured debt, which occurs under predictable financial conditions in the financial life of a firm,<sup>58</sup> payment system users may employ a form of payment in less predictable circumstances. These differences among payment system users complicate efforts to make reliable generalizations about the expected costs and benefits of a payment rule across payment systems. For this reason, Article 9 cannot serve as precedent for a uniform law of payment systems.

### B. *Avoiding Confusion*

Uniformity may also be advocated as a means of avoiding confusion among payment system users.<sup>59</sup> The argument is predicated on a contention that different payment systems should be governed by the same rules when they are used in the same way and as part of the same type of underlying transaction. The similarity in use of payment instruments in part determines the proper extent of uniformity in rules.<sup>60</sup> For instance, credit and debit cards both are used to pay merchants, and most credit card holders apparently do not run ongoing credit balances, although the great majority of outstanding credit card debt at any given time is associated with revolving debt.<sup>61</sup> Thus, if we look at credit card use, as opposed to the amount of debt that is associated with that use, consumer credit cards may be said to be equivalent to debit cards in the underlying transaction of purchase.<sup>62</sup> Consumer users generally will be unaware of the different legal consequences attached to the respective cards. Some cards add to the confusion because they can be used to initiate either a debit or a credit transaction, with the choice potentially made by someone other than the consumer. Accordingly, with respect to payment system rules bearing on the underlying transaction, the rules for consumer credit and debit cards should be the same.

58. See, e.g., Claire A. Hill, *Is Secured Debt Efficient?*, 80 TEX. L. REV. 1117, 1118 (2002); Allen N. Berger & Gregory F. Udell, *Collateral, Loan Quality, and Bank Risk*, 25 J. MONETARY ECON. 21, 23-24 (1990).

59. See, e.g., Mann, *supra* note 4, at 655-56.

60. For Mann's qualifications, see *id.* at 669-70.

61. See Kathleen W. Johnson, Bd. of Governors of the Fed. Reserve Sys., *Convenience or Necessity? Understanding the Recent Rise in Credit Card Debt* 1-3 (Fin. & Econ. Discussion Series, Staff Working Paper No. 2004-47, 2004), available at <https://www.federalreserve.gov/PUBS/FEDS/2004/200447/200447pap.pdf>.

62. Note that we are not saying that this is the appropriate way to look at the issue. It would be perfectly logical to consider the amount of debt, rather than the number of users of credit cards, in order to determine whether credit card use should be considered primarily a convenience device or a borrowing device and to structure the related legal rules.

At the outset, it is notable that there is an anomaly about this argument: standing alone, it is agnostic about the substance of the rule that governs the transactions. What is important is uniformity. Thus, for instance, in the context of reversibility, it does not matter for purposes of the “same payment function, same payment rule” principle whether the uniform rule should (1) allow all cardholders to assert against issuers the defenses they have against merchants, or (2) prohibit all cardholders from raising these defenses. It is partially for that reason that the principle of equivalent function seems to be a questionable basis for justifying uniformity. The principle is insensitive to factors bearing on the optimal allocation of relevant payment risks. If the factors underlying optimal risk allocation for each payment system happen to dictate the same loss-allocation rule, then uniformity would be appropriate. But uniformity would be appropriate as a by-product of the fact that the same risk allocation is optimal for each system, not as an independent objective, to be pursued regardless of its consequences for optimal risk allocation.

Anomaly aside, the argument from confusion ultimately falters on more direct grounds. Payment system diversity imposes two kinds of costs related to confusion. First, it imposes learning costs on those who consider the possibility that different rules will apply and wish to dispel confusion. Second, it imposes error costs on those who are unaware of or miscomprehend the various legal rules that accompany different payment systems and who find themselves bound by legal rules that they did not anticipate. We refer to the combination of learning costs and error costs as “confusion costs.” Of course, any costs imposed by confusion must be weighed against the benefits that payments diversity confers. As we have argued throughout this Article, alleviating confusion through uniform rules may require allocating risks in an otherwise suboptimal way. If payments diversity permits parties to select at low cost a payment mechanism that reflects the best risk allocation for their transaction, then any learning or error costs related to confusion or its avoidance may be swamped by the costs related either to inefficient risk assignments or to the transactions costs involved in bargaining away from the uniform default. We have no definitive answer to this empirical issue. Nevertheless, a variety of considerations suggest to us that the risk of substantial confusion from an ideal level of payments diversity is sufficiently low that concerns for learning and error costs do not warrant full uniformity.

Current law, at least occasionally, appears to recognize this balance. There are cases under current law in which confusion costs could be high. But current law has already adjusted for those situations, even at the risk of compromising desirable payments diversity. The primary example can be found in the treatment of debit cards. Debit card transactions come in two forms: those predicated on a PIN that is processed electronically, and those predicated on a signature that may be processed “offline” in a manner that corresponds to the processing of traditional credit card transactions. The Electronic Fund Transfer Act (EFTA) governs the rights of consumers who engage in electronic fund transfers, and defines those transactions as “any transfer of funds . . . which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape.”<sup>63</sup> Regulation E of the Federal Reserve Board, however, provides a more expansive definition. It includes within the scope of “electronic fund transfer,” any transfer “resulting from debit card transactions, whether or not initiated through an electronic terminal.”<sup>64</sup> The effect of Regulation E is to subject offline debit card transactions to the liability and error resolution schemes of the EFTA, even where no electronic communication is involved. The justification for the expansion lies largely in the risk of confusion from more rigid distinctions among payment mechanisms. Users of debit cards are unlikely to consider the possibility that cards that have the same financial effect—prompt withdrawal of funds from the user’s bank account—will be accompanied by different legal consequences depending on what will seem to the user to be an irrelevant consideration, that is, whether the merchant secured authorization for the transaction by requesting the cardholder to provide a signature or a PIN.<sup>65</sup> The distinction that triggers the application or avoidance of the formal definition of an electronic fund transfer—the process by which the seller collects payment—is both hidden from and irrelevant to the cardholder. Thus, the cardholder is likely to be unaware of and confused by the legal distinctions. Indeed, consumer confusion is likely to be even greater where the same debit card can support both PIN- and signature-based card transactions.<sup>66</sup> Thus, even if the risks associ-

63. 15 U.S.C. § 1693a(6) (2000).

64. 12 C.F.R. § 205.3(b)(v) (2007).

65. Electronic Fund Transfers; Final Rule and Update to Official Staff Commentary, 49 Fed. Reg. 40,794, 40, 794–95 (Oct. 18, 1984) (to be codified at 12 C.F.R. pt. 205).

66. See Julia S. Cheney, Fed. Reserve Bank of Phila., *An Update on Trends in the Debit Card Market 2* (Fed. Reserve Bank of Phila. Payment Cards Ctr., Discussion Paper No. 07-07, 2007), available at <http://ssrn.com/abstract=1007276> (reporting that 85% of debit cards now offer both signature and PIN authorization capabilities).

ated with signature- and PIN-based systems might otherwise warrant different risk allocation rules, such as different rates of fraud,<sup>67</sup> or different processing costs,<sup>68</sup> the confusion costs related to imposing legal distinctions between the systems will likely be sufficiently great to warrant applying the same rules to both. And that is exactly what the current regulations provide.

Other examples of similarly obvious risk of confusion, however, are difficult to identify. True, at some level of abstraction users of payment systems might be confused about the application of different legal regimes to different payment systems. Thus, a user might protest that he or she had no expectation that rules governing risk allocations with respect to checks would be different from rules governing risk allocations with respect to currency, since both deal with forms of payment. But the apparent dissimilarities among different payment systems should often be sufficient to place even untrained users on notice that rules could vary. Our claim, however, is not that payment system users should be charged with notice of the law. Rather, our claim is more pragmatic and empirical: given the obvious differences in payment systems, significant confusion is unlikely to materialize outside the debit card arena where it has been properly addressed. As our summary of current risk allocation suggests, a payment system predicated on allocating losses to parties in the best position to avoid them will likely be characterized by substantial similarity, because the party in the best position to avoid a particular risk with respect to one payment system will also likely be in the same position with respect to other payment systems. If, for instance, payment system users are best positioned to detect and provide notice of the theft of cash and checks, they are also likely frequently to be best positioned, relative to other parties to the transaction, to detect and provide notice with respect to theft of credit cards and debit cards. Thus, we would expect obligations to provide notice to be similar among all these systems. Some differences in timing might be expected, but they will come into play only on rare occasions, since most payment system users are likely to notice large discrepancies in their account shortly after being defrauded and

67. Signature-based debit cards appear to be more vulnerable to fraud than PIN-based debit cards. According to Victor Lubasi, PIN-based debit card fraud losses amount to 0.022% of the value of transactions, and signature-based debit card fraud losses amount to 0.026% of the value of transactions. Victor Lubasi, *Debit Card Competition: Signature Versus PIN*, CHI. FED LETTER (Fed. Reserve Bank of Chi., Chicago, Ill.), Dec. 2005.

68. *See id.*

within the period allotted for notice in all payment systems. As a result, opportunities for confusion will tend to be minimal.

As we indicated at the beginning of this section, one plausible area of confusion that the law does not currently unify involves credit cards and debit cards. The cards look identical in many respects, and are used in similar ways, such as by providing account numbers and expiration dates to the representative of a seller or typing the same information into a website. Transactions involving cards tend to be susceptible to monitoring in the same way, through maintaining physical possession of the cards and inspecting statements for unauthorized transactions. Indeed, some cards may be used for both credit and debit transactions. While the cardholder's selection of the desired type of transaction might be a signal that different legal rules flow from the choice, it would not be unreasonable for a consumer to believe that his or her choice affected only whether an immediate debit was made from a demand deposit account. Thus, the similarities could lull a cardholder into the belief that both types of transactions are covered by the same legal rules.

The rules relating to credit and debit cards diverge in two of the areas with which we are concerned in this Article. The first is the area of "unauthorized use." The second is the area of reversibility. With respect to the first, we anticipate that confusion costs will be quite low. One source of divergence in this area is that the definition of "unauthorized use" differs in each setting. We have indicated above that the divergent definitions of "unauthorized use" may be a function of legislative inattention or drafting inconsistency rather than anything related to the different risks presented by the different systems. If that is the case, then the costs related to confusion should certainly trump the causes of rule diversity. We see little reason not to make the definitions uniform. Here, however, confusion costs are likely to be very small. We anticipate few instances in which implied or apparent authority—the predicate for the broader credit card liability—is present, but actual authority is not. Our examination of the current case law reveals few reported instances in which consumer liability for third-party use of a credit card has rested on the presence of implied or apparent authority and that would likely have been decided differently had the debit card standard been applied. Most "apparent authority" cases have involved firms whose employees had fraudulently obtained credit cards in the name of their employers, and the employers failed to detect the im-

proper use made of the cards notwithstanding the receipt of statements indicating the employees' misfeasance.<sup>69</sup>

The rules for credit cards and debit cards also diverge with respect to the consequences, as opposed to the definition, of unauthorized use. As we have explained above, credit card users face less liability than debit card users in situations where the cardholder has failed to give the card issuer notice of unauthorized transactions. In both cases, the cardholder is liable for unauthorized use of a card only if the card is an "accepted" card, the liability is not in excess of \$50, and the cardholder has notified the card issuer of the loss of the card or unauthorized use.<sup>70</sup> But differences appear where notice is not forthcoming. With respect to credit cards, cardholders bear a maximum of \$50 liability until the card issuer has been notified that an unauthorized use has occurred. The rules are more complicated in the case of debit cards. The \$50 liability cap may be exceeded, first to \$500, and then to an unlimited amount, if the consumer fails to notify the financial institution within relevant time periods that an unauthorized transfer has occurred.<sup>71</sup> This is a distinction with a difference and could generate confusion costs to cardholders unaware of the difference.

But the presence of confusion costs does not mean either (1) that confusion costs are unjustified, or (2) that they can easily be eliminated by a uniform legal rule. With respect to the possibility that the costs are justified, note that the different functions of credit and debit cards expose cardholders and card issuers to different risks. Credit cards expose the party bearing the risk of unauthorized use to the full amount of the account credit limit, which will likely exceed the amount of the cardholder's assets that the card issuer holds. Unauthorized use of debit cards, however, will expose the party bearing that risk only to the amount available in the cardholder's account, though some overdraft privileges may be available. These different risks may warrant different risk allocations. The decision to cap cardholder liability, even when notice has not been given, may reflect a belief that, by determining that the cardholder deserves credit in excess of available assets, the card issuer has indicated its capacity to monitor use of the card and its

69. *See, e.g.*, *Minskoff v. Am. Express Travel Related Serv. Co.*, 98 F.3d 703 (2d Cir. 1996); *DBI Architects, P.C. v. Am. Express Travel Related Serv. Co., Inc.*, 388 F.3d 886 (D.C. Cir. 2004). For a rare case in which an individual was deemed to have given apparent authority for credit card use, see *New Century Financial Services, Inc. v. Dennebar*, 928 A.2d 48 (N.J. Super. Ct. App. Div. 2007).

70. 15 U.S.C. § 1643(a)(1) (2000); 15 U.S.C. § 1693g(a).

71. 15 U.S.C. § 1693g(a).



superior ability to enforce authorization requirements against merchants who accept the card from unauthorized users. The debit card holder, on the other hand, arguably already has significant incentives to protect the assets in his or her related account. Thus, the customer may be expected both to provide prompt notice and to suffer the risk of failing to do so.

Second, alleviating confusion costs between credit cards and debit cards could increase confusion costs with respect to other payment systems. Assume that debit card rules concerning notice and liability were more consistent with credit card rules. That might reduce confusion costs for those who identified credit cards and debit cards as similar forms of payment. But that is not the only parallel that one might draw from an examination of different forms of payment. It is equally plausible that a payment system user would equate debit cards and checks. Both those forms of payment involve direct debits from the customer's checking account that are made with presentation of the authorization (in paper or electronic form) to withdraw funds from the account. Thus, an informed customer might expect the legal rules on unauthorized withdrawals from checking accounts to be the same regardless of form. The structure of the notice and liability schemes for debit cards and checks do tend to be consistent, though not identical. In each case, the customer bears no liability for future unauthorized transactions once the bank is placed on notice of existing or potential misuse, but bears liability up to the amount of the improper withdrawals in the event that the customer fails to detect the unauthorized withdrawals after the bank provides a record of the transaction and after some period in which unauthorized debits should have been detected. The time periods that trigger liability for the different systems vary, and arguably warrant more uniformity, but the basic scheme does not. As a result, efforts to make the debit card liability system more like the credit card system would detach the links between debit card and check liability systems.

The argument for avoiding confusion is no less problematic in the case of reversibility. Credit card rules allow the cardholder a limited right to assert against the card issuer claims or defenses that the cardholder has against the merchant that accepted the card in payment. Debit cards, even debit cards used in a manner that creates an overdraft, entail no such right.<sup>72</sup> Again, at least one form of the argument

72. See 12 C.F.R. § 226.12(c).

for uniformity begins with the proposition that users of credit and debit cards use their cards interchangeably. That is, many credit card users do not necessarily use their credit card as a source of credit, since they pay the balance in full on a monthly basis (although, again, the great majority of outstanding debt represents revolving rather than convenience use).<sup>73</sup> Thus, the argument goes, credit card users will be surprised to learn that the rights that they have with respect to reversing credit card transactions do not equally apply to debit cards.<sup>74</sup>

This argument gives rise to at least two objections. First, it assumes that credit card users will be aware of the credit card reversibility rule, and thus will use it as a baseline for “similar” debit card transactions. Unlike the case of unauthorized use rules, which card issuers advertise in order to induce cardholders to take advantage of “zero liability,” we are dubious that most credit card users are aware of the right to assert against the issuer claims that they have against the merchant. Indeed, it is equally plausible that consumers believe that the baseline rule is that they must pay their credit card issuer and seek recourse against the merchant. The question is an empirical one to which we have no definitive response. But we note that credit card issuers do not appear to advertise the “third-party defenses” right in the same manner that they advertise “zero liability.” If consumers are unaware of their legal rights with respect to either credit or debit cards, there is little reason to suspect that consumer confusion involves disappointment that debit cards do not follow the credit card rule, or happy surprise that credit cards do not follow the debit card rule. It would, of course, be better if cardholders were aware of their legal rights. Our claim is not that we benefit from consumer ignorance. Our claim is only that the current state of consumer knowledge suggests that confusion is not the problem.

The second objection to the confusion argument is that, as in the case of unauthorized use, the same risk in different payment systems entails different costs, so that there is little reason to confront that risk with a uniform rule. In the case of reversibility, the related costs involve the extent to which reversibility requires incurring the costs of a completed transaction. It is technically correct that both credit card

73. See Mann, *supra* note 4, at 656 n.107 (citing CARDDATA, BANK CREDIT CARD CONVENIENCE USAGE—CURRENT, available at [http://www.cardweb.com/carddata/charts/convenience\\_usage.asp](http://www.cardweb.com/carddata/charts/convenience_usage.asp) (subscription required)).

74. See, e.g., *id.* at 634.

and debit card transactions can be undone, but that does not mean that the processes are identical. In the case of a credit card, reversing the transaction will mean undoing a chain of debits and credits between the merchant and the card issuer. It typically will not, however, mean undoing the flow of funds between the credit card holder and the card issuer, as long as the dispute arises prior to the time the cardholder paid the card issuer with respect to the transaction. Thus, the cardholder has always maintained the funds reflecting the purchase price in the disputed transaction over the course of the dispute. In a debit card transaction, however, the cardholder's account will already have been debited the amount of the purchase price. The current reversibility rule for debit cards leaves those funds with the merchant. Reversing the transaction requires undoing the transfer from the cardholder's account as well as the transaction between the card issuer and the merchant.

Is that step sufficient to shift the balance of costs and benefits? That seems unlikely in a computerized age. But the additional step reveals an additional significance to the distinction between credit cards and debit cards, and one that may be worth retaining. In each case, current law imposes on the party who seeks the funds the burden of litigation to recover the purchase price. Thus, the question is whether a single reversibility rule for both credit and debit card transactions optimally allocates the litigation burden between the cardholder and the merchant. The longstanding rule for irreversibility with respect to cash transactions suggests that there may be some value in allowing parties to structure their dealings in a manner that allocates the burden to the party who has parted with funds, notwithstanding the technical feasibility of returning the cash. For instance, no technical infeasibility precludes a rule that requires merchants to return cash to consumers pending the outcome of a dispute. Our unwillingness to apply such a rule implicitly recognizes either that the related costs are too great, or that the probabilities with respect to outcome on the merits favor the merchant and thus places the litigation burden on the party whom we believe is likely to lose.

As we discuss below, it is not clear whether such an implicit conclusion is justified. We are not aware of the rate at which disputes between consumers and merchants are decided on the merits in favor of the former. There are reasons to think that merchants will avoid dispute-producing behavior, both because of their relationships with card

networks and their reputational stake in satisfying card holders.<sup>75</sup> On that rationale, it is the credit card rule that appears anomalous. Our point here, however, is not that either the credit card rule or the debit card rule is the correct one. Rather, our limited point in this section is to demonstrate that, given plausible arguments for each, a menu approach that reflects either different costs or, where costs are unclear, different choices, may be preferable to imposed uniformity. That choice entails potential for residual confusion may be a call for conveying better information to consumers, but is not necessarily a justification for dissolving the relevant distinctions.

Finally, reversibility poses the problem that resolving potential confusion between credit cards and debit cards risks exacerbating confusion between debit cards and checks. A consumer who used a check to pay for the defective transaction, or who removed cash from his or her checking account, would have had no right to assert against the bank any claim or defense valid against the merchant once the payment was final. The debit card, which accesses the same demand deposit account, retains the same principle. It simply expedites the time of final payment relative to a check. But given that a consumer could understand that debit cards and checks are equivalents for purposes of gaining access to a demand deposit account, making debit card rules parallel to credit card rules could cause confusion costs for consumers no less than the confusion costs created by distinguishing between credit cards and debit cards for purposes of notice or reversibility.

Of course, the natural response is to contend that confusion in either case could be alleviated if all three payment systems (credit cards, debit cards, checks) were governed by the same rules. But to say that is to suggest that the risks aligned with all three systems are equivalent and that users would not benefit from having a choice among systems that allocate risks differently. We have suggested that there may be reasons to distinguish among these systems, based on superior risk-bearing potential. We extend that argument in the next Part of this Article. For the moment, we suggest only that confusion costs, standing alone, do not justify uniform treatment of payment systems. Parties to payments transactions presumably would incur some confusion costs if doing so minimized other risks of greater value. There is little reason

75. See Mann, *supra* note 4, at 661–62.

for the law, in the name of uniformity, to create default rules that vary from the rules for which most parties would bargain.

*C. Eliminating Distortion from Legal Rules*

Another principal argument offered for uniformity is that the presence of different legal rules for different forms of payment distorts choice among payment systems.<sup>76</sup> If the same risk (e.g., fraud in the payments system or in the underlying transactions) is present across payment systems, and if payment system users and providers are similarly situated with respect to them, the allocation of the risk should be the same across payment systems. Legal rules that assign the relevant risk differently create different costs for using different forms of payment. If the relevant risk across payment systems is the same, a divergence between legal rules biases the choice of payment system unrelated to the costs created by the rules. Uniformity in payment system rules allegedly eliminates those costs.

A standard illustration of this phenomenon involves the different legal rules pertaining to the unauthorized use of checks and debit cards. The person in whose name a check is issued is liable for the amount of a forged check if the making of the unauthorized signature is the result of that person's negligence.<sup>77</sup> By contrast, unless otherwise provided by contract, the non-consumer debit cardholder is liable for debits resulting from use of its debit card. The cardholder's liability is limited by the amount of the balance in the debited account, plus any overdraft privileges that the unauthorized user can exploit. If the debit cardholder is a consumer, he or she is liable for no more than \$50, assuming timely notice of unauthorized use, even if negligent with respect to the use.<sup>78</sup> Assuming that the risk of unauthorized use is the same for checks and debit cards, and that users of checks and debit cards have the same capacities to control against unauthorized use,

76. See SCOTT, *supra* note 54, at 39–40; UNIF. NEW PAYMENTS CODE (Permanent Editorial Bd. for the U.C.C., P.E.B. Draft No. 3, June 2, 1983); Miller, *supra* note 51, at 1216.

77. See U.C.C. § 3-406(a) (2005). Is that person a drawer of the check? Arguably, yes. A “drawer” is person “who signs or is identified in a draft as a person ordering payment.” U.C.C. § 3-103(a)(5). The person whose drawer's signature is forged on a check is “identified” as a person ordering payment. Perhaps the “identified” language was meant only to cover agency relationships, not unauthorized signatures. However, at least one court has classified the person whose signature was forged as a drawer, and thus precluded that person from bringing a conversion action under U.C.C. section 3-420(a). See *Borg v. Chase Manhattan Bank USA, N.A.*, 247 F. App'x 627 (6th Cir. 2007).

78. 15 U.S.C. § 1693g(a)(1) (consumer's liability not to exceed the lesser of \$50 or the amount of the property or services obtained in the transaction).

different rules concerning unauthorized use distorts the user's choice of payment by check or debit card.

The choice among payment instruments governed by different rules raises two different questions. One is whether the difference in rules distorts the choice of payment instrument. Here, we assume that the parties are aware of the different legal rules, since distortion can occur only if the selection is made on the basis of the legal differences. This assumption, we suspect, is highly counterfactual, as we surmise that the great majority of payment system users are unaware of the legal consequences of their choices. Nevertheless, we are willing to make the assumption in order to test the distortion argument. The second question is whether the difference is justified by overriding considerations, even if the distortion exists. Take the questions in turn. First, is there in fact a "distortion" in the choice of payment instrument that uniform rules need to address? The answer to that question, in turn, depends on the relevant risks allocated by different legal rules being equivalent. Different rules in payment systems distort choice only if the risks and capacities for controlling them are the same across payment systems. If the selection among payment instruments is the consequence of a reaction to different risks, then the opportunity to select among instruments may actually lead to optimal risk allocations, rather than to a socially undesirable distortion. Thus, before we can confidently conclude that check writers and card holders are similarly situated with respect to unauthorized use of their payment systems, we would want to know the risks they face, the average size of the withdrawal made through each system and the variance around that mean when that risk materializes, and the costs of avoiding risks within each system.

To continue our example of checks and debit cards, it seems apparent that the risks of using these different mechanisms are not equivalent. Consider the drawer and non-consumer debit cardholders' respective losses when negligent. Safety, record keeping, budget control, negotiability, and the float make checks a preferred means of making large dollar payments.<sup>79</sup> Debit cards, by contrast, typically are used to make smaller dollar payments;<sup>80</sup> the average value of debit card

79. See Garcia-Swartz et al., *supra* note 50, at 188-91; David B. Humphrey, *Payment Systems: Principles, Practices and Improvements* (World Bank, Technical Paper No. 260, 1995).

80. In 2003 the average value of checks was \$1,065; in 2000 it was \$951. Geoffrey R. Gerdes et al., *Trends in the Use of Payment Instruments in the United States*, 91 FED. RES. BULL. 180, 182 (2005). Checks remain the most common form of non-cash payment instrument by value, excluding wire transfers. *See id.* at 181 & n.6.

payments in 2003 was \$40.<sup>81</sup> The average loss in a check fraud case in 2003 was \$1098.<sup>82</sup> At the same time, the average value of losses per debit card fraud case was \$294 for signature debit cards and \$371 for PIN-based debit cards.<sup>83</sup> We also suspect that the rate of fraud is lower for debit card transactions than for checks. The 2004 ABA Deposit Account Fraud Survey Report notes that banks surveyed in 2003 reported one loss claim per 29,923 debit card transactions.<sup>84</sup> While we have been unable to find reliable comparable figures for checks, there is anecdotal evidence that fraud rates are higher. During that same period, 36.6 billion checks were written.<sup>85</sup> The ABA Deposit Account Fraud Survey Report received survey forms from 417 of the 5,081 banking institutions to which forms were sent.<sup>86</sup> These 417 institutions alone reported 616,469 check fraud cases.<sup>87</sup> Assuming they were representative, the 5,081 recipients of the survey would have suffered approximately 7.5 million instances of check fraud for a ratio of one fraud claim for every 4880 checks. In addition, banks report much greater concern about check fraud than debit card fraud.<sup>88</sup>

Risks also arise from very different sources for checks and debit cards. Debit card fraud arises from the theft of the physical card, a related access device such as a PIN, or both. Check fraud arises from forged indorsements, forged drawer signatures, counterfeiting, alteration, and check kiting schemes. This combination of different expected losses and different sources of unauthorized use suggest that cost-justified loss avoidance measures will also differ, both for payment system users and payment system providers. The higher average value of checks, for instance, may justify a drawee bank in honoring a check of a certain amount without undue suspicion, while a debit card transaction of the same amount might raise questions, especially if banks have the capacity to track the spending patterns of their customers. Some of these differences may result from the fact that debit cards are more likely to be used by consumers, while businesses may continue to be users of checks. It is, therefore, plausible that we would want differ-

81. *Id.* at 183; Cheney, *supra* note 66, at 3. They are the most common instrument used to make small-value payments, except for cash. Gerdes et al., *supra* note 80, at 183.

82. AM. BANKERS ASS'N, ABA DEPOSIT ACCOUNT FRAUD SURVEY REPORT 13 (2004).

83. *Id.* at 41.

84. *Id.*

85. *See* Gerdes et al., *supra* note 80, at 181.

86. AM. BANKERS ASS'N, *supra* note 82, at 3.

87. *Id.* at 13.

88. *See id.* at 11.

ent rules for consumer and non-consumer payment system users. We explore that issue below. At this point, we note only that the underlying assumption of the distortion argument, that is, that superficially similar payment systems present similar risks that will be distorted by dissimilar legal rules, is highly suspect. There is little reason to conclude that the optimal rule for unauthorized use will be uniform for checks and debit cards.<sup>89</sup>

The second question is whether overriding considerations justify different legal rules across payments instruments even if they distort choice. The argument from distortion assumes that distortion in the choice of payment instrument justifies the uniform rules across payment systems. The assumption is unsound. Attitudes toward risk might justify different legal rules, even if the expected value of fraud losses were the same across payment instruments. Consumers, for instance, might be risk-averse over some outcomes. In transactions where such outcomes are possible, they might prefer to allocate the relevant risk to another party. Diversity in rules allows risk-averse consumers to select easily the payment instrument suitable for them. For instance, the effective zero liability for a debit card may be appealing to a consumer who is risk-averse with respect to unauthorized use. Such a consumer may prefer to pay by debit card rather than by check, even if debit card transactions require payment of a risk premium. Accordingly, the different limits might justify different loss-allocation rules for debit cards than for checks issued by consumers.

### III. OPTIMAL STANDARDIZATION IN PAYMENT SYSTEMS

#### A. *General Principles*

We suggested at the outset that parties who use payment systems might prefer diversity in legal rules rather than uniformity. Our rationale is that parties to different transactions, or different types of parties in similar transactions might prefer to allocate risks differently. A menu of legal rules allows parties to structure their transaction at the lowest possible cost by selecting a payment system that best approximates their optimal allocation of the legal risks that attend payment. This is not to say, however, that current payments rules or payment systems achieve the optimal level of diversity.

89. Cf. Gillette, *supra* note 9, at 223-25 (making point in connection with liability limits on checks and credit cards).



Notwithstanding our view that parties might have different preferences about how to allocate the payment risks in a particular transaction, we believe that they would share a common view about what the legal rules of each payment system should accomplish. The law of payment systems is composed primarily of default rules; parties could, for the most part, redefine the risk allocation created by the legal rules. Presumably, therefore, the legal rules that govern any payment system should reflect the preferences of most parties who use that payment system. Legal rules that reflect majoritarian preferences minimize the costs that must be incurred to complete that transaction, because most parties do not need to negotiate about the legal rules. They can simply adopt the state-supplied default rules. Only idiosyncratic parties will be required to negotiate around the defaults.

We further assume that, in most cases, parties to any payment system would prefer legal default rules that allocate any risk to the party in the best position to avoid it. Basically, that requires placing the loss on the party who can minimize the sum of loss avoidance costs and residual losses that remain even once cost-effective precautions are taken. That principle, well recognized in the literature<sup>90</sup> and case law<sup>91</sup> on payment systems, minimizes transactions costs, because allocation of a risk to an inferior risk bearer will require that party to charge costs for risk bearing that could be reduced if the risk were assigned to the superior risk bearer. A legal rule that placed the loss on the superior risk bearer would avoid the costs of contracting around the inefficient rule or of absorbing excess social losses due to friction in the contracting process. The law with respect to fraudulent signatures on checks appears most explicitly to adopt this rationale. The current interplay of bank liability for unauthorized payments, unless the person asserting lack of authority was himself negligent or could more readily monitor the wrongdoer, is best explained as embodying a system in which losses are allocated to the party in the best position to avoid them.<sup>92</sup>

90. See, e.g., Edward Rubin, *Efficiency, Equity and the Proposed Revision of Articles 3 and 4*, 42 ALA. L. REV. 551, 566–67 (1991).

91. See, e.g., TD Banknorth, N.A. v. Keybank, N.A., No. 05-180-P-H, 2006 WL 1554712, at \*\*5–6 (D. Me. June 2, 2006); Washtenaw Mortgage Co., Inc. v. Nat'l City Bank, No. 04-239-JBC, 2006 WL 1207651, at \*2 (E.D. Ky. Apr. 28, 2006).

92. See U.C.C. § 3-405 cmt. 1 (2005) (explaining “employee responsibility” rule as “based on the belief that the employer is in a far better position to avoid the loss by care in choosing employees, in supervising them, and in adopting other measures to prevent forged indorsements on instruments payable to the employer or fraud in the issuance of instruments in the name of the employer”).

The assumption that most participants in a payment system would prefer to allocate losses to the party in the best position to avoid them needs careful statement. It requires a full understanding of what it means to be in a superior position to avoid a loss. One party can be in a superior position to avoid one element that contributes to the loss while another party is better positioned to avoid another element of it. Further, a party may be in an inferior position to avoid risks given current technology, but be in a superior position to develop new technology that avoids or reduces loss.<sup>93</sup> Alternatively, informational asymmetries may mean that one party is well positioned to take precautions against a loss, but another party has superior information that is necessary to determine the expected value of taking those precautions. In such a case, it would be desirable to have a legal rule that induced the party with superior information to convey it to the uninformed party or to develop precautionary measures that can be utilized by the less informed party. For instance, banks, as repeat players in the payment system, will have superior information relative to any given customer about schemes used to defraud individual customers. Bank customers, on the other hand, are in a superior position to take certain precautions that will protect their accounts against theft or fraud. Placing the loss of fraud on banks induces them to invest optimally in creating fraud detection and deterrence methods that can best be implemented by customers. These include issuing warnings about false keypads at ATM machines, the installation of mirrors and security at ATM machines, recommendations for “commercially reasonable” security procedures for wire transfers, and positive pay systems for checks. Thus, with respect to these risks, legal rules should induce banks to take fraud detection and deterrent measures that they are best able to implement, and should induce customers to take those precautions that they are best able to implement. But the contingent nature of the desirable precautions and technological development make it unlikely that the same party will have a comparative advantage with respect to all relevant losses or across all payment systems.

The majoritarian preference for optimal risk allocation is subject to two caveats. First, some parties to transactions that involve payment systems may be averse to certain risks and thus prefer to shift related losses to other parties, regardless of who is in a superior position to avoid the loss. For instance, individuals, such as consumers or sole proprietors, may be more concerned with loss avoidance than with

93. See Mann, *supra* note 4, at 638.

optimal risk bearing, and the law is perhaps more likely to be responsive to issues of risk aversion in the case of individuals.<sup>94</sup> Risk-aversion, however, is not limited to individuals. Firms insure against some risks even when not required by regulation or rules of corporate governance, and some individuals forgo insurance. Nonetheless, consumers probably are more frequently averse to risk than firms. Equally as important, being a consumer is a more reliable and less manipulable characteristic better correlated with attitudes toward risk than easily verifiable characteristics of firms. If parties other than consumers are reliably and easily identifiable as risk-averse, payment rules allocating loss may reflect their preference that risk be shifted away from them.

The second caveat is that, notwithstanding the general desire to minimize the sum of losses and loss avoidance in any payment system, there may be circumstances under which other objectives trump efficient risk bearing. As we discuss below, these objectives may address distributive concerns, where it can be demonstrated that efficient risk allocation systematically places losses on a social group that we desire to protect from risk bearing. Indeed, under those circumstances, it is possible that the socially optimal rule would be a mandatory rule that is imposed uniformly across the payment systems used by the group to be protected.

This Part argues that the factors that determine optimal risk bearing do not readily lend themselves to the identification of a single majoritarian default rule for all payment systems. Those factors may point to different risk bearing advantages in different transactions and for different transactors. Under these circumstances, parties to transactions may prefer a menu of risk allocation rules from which they can select one that best approximates their risk preferences to a single rule around which significant bargaining must occur. In what follows, we consider a variety of different risks and demonstrate the difficulty of deriving a single optimal default. The consequence is that variety in the legal rules that allocate these risks may be superior to uniformity. That is not to say that the current level of legal variety is itself optimal. Indeed, throughout this section, we suggest how current law deviates from what we would consider an optimal level of diversity in payments rules. It is only to say that uniformity is not necessarily the cure for suboptimal variety. The remaining sections of this Part argue that diverse payments rules can better allocate relevant risk.

94. The market for managers and the presence of competition among firms suggest that there is less reason for legal intervention to address risk aversion in that context.

### B. *Unauthorized Payments*

The possibility of fraudulent or unauthorized use constitutes one of the major risks that attend any payments system. Our assumption that commercial law should do for the parties what they would otherwise do for themselves suggests that uniform treatment of fraud risks may be appropriate at a high level of generality. That is, consistent with the common understanding that legal rules should minimize the costs of payment systems, each system should allocate the loss of unauthorized use to the party in the best position to avoid it. As noted above, left to their own devices parties would likely bargain to that allocation in order to minimize the total of fraud costs and anti-fraud precautions.

Nevertheless, some of the caveats that we associated with the optimal risk bearing are particularly salient with respect to unauthorized payments. As between the system provider and system user, different parties may be the superior risk bearers with respect to different types of fraud; moreover, a superior risk bearer under one technology may not be the superior risk bearer under an alternative technology, so the identification of the superior risk bearer could be endogenous. In addition, the risk that bank customers may be vulnerable to significant losses as a consequence of unauthorized payments could trigger some of the distributive concerns that justify pursuit of objectives other than superior risk avoiding.

#### 1. Varieties of Fraud and Fraud-Prevention Technologies

Consider the first difficulty. Depository banks are likely best positioned to protect against forged payee indorsements by virtue of their capacity to ensure that checks are only deposited into accounts bearing the payee's name and to monitor the conduct of their customers. Thus, the current legal rule that allows the party whose signature has been forged to recover in conversion from the depository bank makes sense.<sup>95</sup> Moreover, the relative ability of a drawee bank to recover from the depository bank on a warranty theory in such a situation arguably justifies the requirement that the drawer recover from the drawee,<sup>96</sup> while the latter proceeds against the depository bank.<sup>97</sup>

95. See U.C.C. § 3-420(a).

96. An issuer of a check is barred from bringing an action in conversion. *Id.*

97. See U.C.C. § 3-417.

But check fraud law recognizes that one cannot conclude that the depository bank systematically occupies the “superior position to avoid the loss.” Exceptions to bank liability for forged indorsements essentially impose on users of the payment system an obligation to take advantage of low-cost precautions that would reduce check fraud, presumably on the assumption that in some unique circumstances payment system users have an advantage over system providers in detecting and deterring fraud. An employer who fails to monitor employees,<sup>98</sup> a drawer who signs a check without determining that the payee is actually owed money,<sup>99</sup> and a drawer who fails to determine the true identity of an impersonator<sup>100</sup> arguably each stands in a better position than the depository bank to detect and deter fraudulent activity. The argument that the system users, employers in particular, should bear the fraud costs in these situations as a cost of doing business<sup>101</sup> entails the belief that employers can bear these risks at lower costs than depository banks. If that is the case, then a uniform provision that places the loss on system providers would generate excess precaution costs.

The situation becomes more complicated when we turn to forged drawers’ signatures. Here, the law presumptively places the loss on the drawee bank that pays the check. Upstream banks do not warrant to the drawee that the drawer’s signature is authorized.<sup>102</sup> The drawee bank would bear no liability if it detected the forgery prior to making payment on the check, although in practice detection is impractical. The original explanation for the apparent anomaly in making drawees liable for paying checks bearing forged drawers’ signatures, based on technical capacity to compare signatures on checks to those on signature cards and embodied in the chestnut of *Price v. Neal*,<sup>103</sup> retains little persuasive power for most commentators.<sup>104</sup> Few believe that in a technological age banks will or should compare signatures on any but the largest or most suspicious checks with those on customer signa-

98. *Id.* § 3-405(b).

99. *Id.* §§ 3-404(b), 3-406.

100. *Id.* § 3-404(a).

101. *See id.* § 3-405 cmt. 1.

102. *See id.* § 3-417(a)(3) & cmt. 3.

103. (1762) 3 Burr. 1354, 1357, 97 Eng. Rep. 871, 872 (K.B.).

104. *See, e.g.*, Christopher M. Grengs & Edward S. Adams, *Contracting Around Finality: Transforming Price v. Neal from Dictate to Default*, 89 MINN. L. REV. 163, 179 (2004) (rule is “not entirely without controversy”); A. Brooke Overby, *Check Fraud in the Courts After the Revisions to U.C.C. Articles 3 and 4*, 57 ALA. L. REV. 351, 360 (2005) (rule now a “quaint historical relic with little practical force in modern banking law”); Rogers, *supra* note 2, at 454.

ture cards. In an age in which counterfeit checks can be processed as facsimiles of originals, comparisons with signature cards will likely reveal no difference to the most highly trained eye.<sup>105</sup>

But here, the second difficulty is present: the identity of the superior loss avoider may change depending on the level of technology assumed. Placing liability on drawees with respect to drawers' signatures does provide an incentive for banks to develop technologies to detect fraud. If drawee banks are better positioned than customers or depository banks to engage in that activity, then the assumed irrelevance of *Price v. Neal* to contemporary banking dissipates. It may be true that drawees cannot efficiently review drawer signatures. But signature comparisons are not the only plausible anti-fraud precaution. For instance, the development of positive pay systems, in which drawees make available to customers a means to designate checks that have been authorized for payment prior to the time of presentment, presumably occurred only because drawee banks could develop and implement such systems at a cost lower than the fraud costs that they would otherwise bear. If customers bore liability, collective action problems among a large, diffuse, and difficult to organize population of bank customers would presumably frustrate any efforts to develop a similar system. Imposing liability on banks in their status as depositaries might also interfere with such technological developments, because when banks act as depositaries they typically bear liability to non-customers whose indorsements have been forged. Depository banks would have difficulty marketing a positive pay system to that population, since the banks are not in a relationship with the potential beneficiaries and could not easily identify the members of that population. The result is that even if a class of actors is not in a superior position to bear losses under the current state of anti-fraud technology, they might be in a superior position to develop a different level of technology. Expecting rules that uniformly allocate losses within and across payment systems under these circumstances is unlikely to serve the objective of minimizing the total costs of fraud and anti-fraud precautions.

Nevertheless, it seems clear that some current payment rules involving unauthorized payments are inconsistent with the objective of loss minimization. Rules that impose liability on card issuers even

105. See, e.g., *Wachovia Bank, N.A. v. Foster Bancshares, Inc.*, 457 F.3d 619, 622 (7th Cir. 2006); *Chevy Chase Bank, F.S.B. v. Wachovia Bank, N.A.*, 61 UCC Rep. Serv. 2d 458, 461 (4th Cir. 2006).

when the cardholder has demonstrably been negligent are unlikely to reduce the total costs of fraud and anti-fraud precautions. For instance, in the case of a consumer who allows a third party to lurk behind him and steal a PIN, who responds to phishing emails that have characteristics indicating their fraudulent nature, or who negligently keeps passwords and usernames in a conspicuous place, subsequent unauthorized access to the consumer's account that is made possible by those actions is still considered unauthorized and chargeable to the financial institution from which the transfer was made. Given that the card issuer will be unable to distinguish the identity thief's use from authorized use, and given that the finding of negligence implicitly suggests that the consumer was in a superior position to avoid the loss, the decision to protect consumers in these situations necessarily deviates from the general proposition that parties to payments transactions would desire to allocate losses in a manner consistent with risk-avoiding capacity.

## 2. Consumer Protection and Diverse Payment System Rules

The case for diversity in payments system rules can be based on two different grounds: optimal risk allocation and non-efficiency goals. Part III.A noted the possibility that uniform rules are inappropriate because different payment systems are intended to serve different objectives. Unauthorized use rules that ignore user negligence arguably reflect a decision to subordinate efficiency in payments law to some other goal. The liability limits in payment systems for credit and debit cards are touted as consumer protection schemes rather than as efforts to place losses on the party in the best position to avoid them. Thus, it makes sense to ask whether payment system rules should be uniform across users, or whether they should distinguish between consumer and non-consumer users. This could be done either on a case-by-case basis, so that the same payment system is subject to different rules depending whether the user in the particular case is a consumer or a non-consumer. Or we could have different rules apply to different systems, depending on whether the system tends to be dominated by consumers or non-consumers. We argue below that consumer protection does not justify deviation from the objective of optimal risk allocation. Thus, notwithstanding our general proposition that variety among payment systems is useful, the consumer area may be one in which there is insufficient uniformity with non-consumer payments law. It is plausible, however, that behavioral characteristics of consum-

ers would justify legal restrictions that augment payments law, such as disclosure requirements and limitations on clauses. Doing so, however, is best justified not because “consumer protection” warrants deviation from the standard objectives of payments law. Rather, such deviations are justified, if at all, because systematic vulnerability of consumers to certain conduct means that they do not occupy the best position to avoid losses.

Note first that, to the extent that payment systems seek to distinguish between consumers and non-consumers, current law creates an anomaly. If the objective is to create a regime of consumer protection that subordinates efficiency concerns, then it is unclear why that objective is not pervasive across payment systems. Checks that are drawn on consumer accounts are subject to the same loss-allocation rules as checks drawn on business accounts. Those rules reduce or eliminate bank liability for fraud where the consumer has been negligent and the bank has not. If the bank that a consumer claims took or paid a check bearing a forgery can demonstrate that the consumer failed to exercise ordinary care in a manner that substantially contributed to the making of the forgery, the bank bears no liability. If the bank itself failed to exercise ordinary care in taking or paying the check, the loss is allocated according to principles of comparative negligence between the bank asserting the preclusion and the person precluded.<sup>106</sup> These rules, of course, stand in contrast to the federal rules that render consumer negligence irrelevant in the case of electronic fund transfers. The anomaly cannot be explained by administrative difficulty in distinguishing between consumer and non-consumer checks in an age where simple MICR coding could identify the nature of each checking account. If consumer protection is the supervening principle for payment systems involving consumer cards or access devices, it is unclear why efficiency principles that place losses on the party in the best position to avoid them should prevail over the same concerns in check systems.

In evaluating the propriety of distinguishing between consumers and non-consumers, we differentiate between two types of pro-consumer regulations. One set purports to compensate for psychological biases and heuristics from which consumers are likely to suffer and that are not readily susceptible to market corrections. Under these circumstances, government regulation may be appropriate to avoid exploitation of consumers who might otherwise accept terms that do

106. See, e.g., U.C.C. §§ 3-404(d), 3-405(b), 3-406(a)-(b).



not reflect either an actual bargain or a virtual bargain of the type that would emerge in the presence of market competition.<sup>107</sup> There is significant and growing literature about measures used by credit card issuers that arguably take advantage of the behavioral limitations of consumer decision making in a manner that might justify legal intervention. Consumers may, for instance, underestimate the likelihood of incurring late fees, defaulting on credit obligations, or suffering adverse consequences by making only minimal payments on outstanding credit card balances. Credit card issuers may respond by imposing interest rate increases or late fees that exceed the increased risk associated with default or late payment. Alternatively, consumers may ignore non-salient clauses in credit card contracts in ways that make them susceptible to supracompetitive prices. For instance, while consumers likely pay attention to interest rates on credit cards, so that different credit card companies compete on that variable in ways that render government regulation superfluous, fees for services such as currency conversion may be less salient at the time the cardholder obtains a credit or debit card or even at the time the cardholder uses the card. As a result, card issuers may be able to charge noncompetitive fees for the conversion service.<sup>108</sup>

There is a useful and robust debate about whether these practices exploit informational asymmetries, high switching costs, or hyperbolic discounting and other cognitive errors by consumers, or whether they are cost-justified responses to signals of higher default risk than was reflected in the original terms on which the credit card was issued.<sup>109</sup> There is also significant debate about whether consumer vulnerability to these practices is persistent, or can be reduced by additional disclosure and other debiasing techniques.<sup>110</sup> The more consumers appear vulnerable to these practices without the protection of traditional competitive restraints on issuers, the stronger the argument for special protection that may deviate from the norm for payment systems. Un-

107. See Clayton P. Gillette, *Rolling Contracts as an Agency Problem*, 2004 WISC. L. REV. 679, 716-21.

108. See, e.g., Samuel Issacharoff & Erin Delaney, *Credit Card Accountability*, 73 U. CHI. L. REV. 157, 161-62 (2006).

109. See generally RONALD J. MANN, CHARGING AHEAD 4-5 (2006); Oren Bar-Gill, *Bundling and Consumer Misperception*, 73 U. CHI. L. REV. 33, 48-49 (2006); Oren Bar-Gill, *Seduction by Plastic*, 98 NW. U. L. REV. 1373, 1401 (2004); Ronald J. Mann, *Regulating Internet Payment Intermediaries*, 82 TEX. L. REV. 681, 692-93 (2004).

110. For analysis of both anti-consumer measures that may survive in a competitive equilibrium and measures that may dissipate over time due to competition, see Xavier Gabaix & David Laibson, *Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets*, 121 Q.J. ECON. 505 (2006).

der these circumstances, government regulation—either in the form of disclosure to correct consumer misinformation, or to substantively regulate services that cannot readily be made salient to consumers—may be appropriate in the name of consumer protection. The recent concerns for consumer vulnerability, however, do not appear to involve rules that vary across payment systems, or that allocate the payment risks with which we are primarily concerned. That is, with one possible exception that we discuss below, rules that allocate risks of unauthorized payment, irreversibility, and payment error are not implicated by the cognitive errors that arguably infect decision making about interest rates and incurring debt. They deal with issues of consumer behavior with respect to known risks, rather than excusable ignorance of unknown risks.

The line between the known and unknown risks certainly is not clear-cut. One might justifiably ask whether consumers who make their PINs easily accessible to others are negligently ignoring salient risks, or are suffering from a bias of underestimating the likelihood that a risk will materialize. Thus, one might claim that the negligence concept is too flexible to permit easy application in the case of consumers, because it cannot accommodate information asymmetries between unsophisticated consumers who are unaware of the risks they create through careless behavior and financial institutions that, as repeat players, have both data and the capacity to inform their customers of the dangers of carelessness. At the time the EFTA was enacted, in 1978, concepts such as PIN numbers and electronic fund transfers at ATMs were relatively novel. In those relatively innocent, pre-identity theft days, it is plausible that many consumers would have been unaware of the risks related to acts such as writing PINs on cards or otherwise making means of account access available to third parties. A broad immunity for negligence avoided *ad hoc* inquiries into the level of care of consumers who were easily fooled into surrendering information to wrongdoers, but who, given the novel state of technology and low level of exposure to risk or information about risk, were unlikely to be negligent in a legal sense.<sup>111</sup> Similarly, at the time that spam emails began, consumers might have been forgiven for responding to fraudulent phishing emails that invited bank customers to change their personal banking information online or to assist in recov-

111. See, for instance, the early cases on ATM misuse, such as *Feldman v. Citibank*, 443 N.Y.S.2d 43, 45 (N.Y. Civ. Ct. 1981), and *Ognibene v. Citibank*, 446 N.Y.S.2d 845, 848 (N.Y. Civ. Ct. 1981).

ering millions from the treasury of a developing nation's former dictator. Avoiding negligence inquiries under those circumstances might be thought of as a means of reducing error costs that would have inevitably arisen as courts and juries sought to determine reasonable behavior under changing circumstances. Strict liability for more informed, repeat player card issuers would have induced them to convey information to consumers concerning appropriate precautions.

The problem with such justifications for different consumer rules is that they rely on a level of information that is likely to evolve over time. While consumers may have been relatively unaware of the risks of failing to protect PINs during the first years of popular ATM withdrawals and debit cards, it is the rare consumer today who is not bombarded with information concerning identity theft and the need to protect financial information. Those who continue to fall prey to email scams or phishing expeditions generate less sympathy than disbelief at their gullibility.<sup>112</sup> The explanation that liability is necessary to induce banks to caution consumers seems outdated at a time when the number of electronic transactions exceeds the number of personal checks, and when consumers increasingly utilize electronic fund transfers from multiple sources—payroll cards, debit cards, computerized payments—that require the use of a PIN or other access device that the consumer understands can permit unauthorized access if misused. To the extent that liability induces banks to provide information to consumers, bank liability for non-negligent unauthorized transfers could be sufficient to encourage an optimal flow of information. Continued excuse of behavior that today appears negligent, therefore, may be more a function of path dependence and the stickiness of regulation than of consideration of the proper scope of consumer protection under current circumstances. If that is the case, then more uniformity than current law provides might be appropriate, but it would be uniformity that avoids current distinctions between consumers and non-consumers.

Moreover, the claim that disregarding consumer negligence serves the objective of consumer protection is itself contestable. We do not propose here to rehearse the arguments for or against fulfilling these objectives through the payment system rather than through broad-based subsidies in the tax system. We do, however, note one overlooked phenomenon of the effort to protect consumers by immunizing

112. See, e.g., *Jimena v. UBS AG Bank, Inc.*, No. 1:07-CV-00367, 2007 WL 1687045, at \*1 (E.D. Cal. June 8, 2007); *Valley Bank v. Hughes*, 147 P.3d 185, 188 (Mont. 2006).

negligence. Ignoring consumer negligence does serve the interests of negligent consumers. Assuming that they were well positioned to avoid losses, shifting those losses elsewhere entails excess costs that likewise must be borne elsewhere. In a competitive environment, one would anticipate that financial institutions will seek to shift the costs of consumer negligence that banks bear as a consequence of consumer immunity back into the consumer banking system through higher fees and charges. As a consequence, non-negligent consumers will bear at least some of the costs related to consumer negligence. It is plausible that non-negligent consumers would prefer to bear lower fees and charges that would flow from optimal risk allocation to the higher amounts that they bear in order to subsidize the negligence costs related to other consumers. If that is the case, it is a peculiar conception of "consumer protection" that requires the subsidy within the consumer class. If we believed that consumer negligence correlated well with subclasses of consumers that systematically needed protection, such as the poor or the elderly, then we might justify the subsidy on distributive grounds. The poor, however, are more likely to fall within the range category of the "unbanked" than within the category of credit and debit card users.<sup>113</sup> In short, absent information about who benefits from immunity for negligence, it is not clear that consumer protection justifies the deviation from the objective of placing losses on the party in the best position to avoid them.

### C. *Diversity by Payments User*

The issue of uniformity becomes more complicated when we ask whether consumers and non-consumers should be distinguished in payment systems that are used by both groups. For instance, one might insist that consumers are poorly served by the Article 3 and Article 4 rules that apply to any check. That claim may be rooted in either of two explanations. First, one might contend that consumers have been excluded from the drafting process that promulgated the rules, and were not represented by any group that was involved. Second, one might contend that consumers have different risk avoiding capacities than non-consumers. Neither of these explanations seems plausible in the context of check rules, however. With respect to the first, it is certainly the case that the original Article 3 and Article 4 rules were drafted primarily by bank interests, with some input from business inter-

113. See Michael S. Barr, *Banking the Poor*, 21 YALE J. ON REG. 121 (2004).

ests.<sup>114</sup> Consumer groups, even the few that may have existed during the period when Articles 3 and 4 were originally drafted, appear not to have been at the table. Consumer groups were more apparent in the 1990 revision of Article 3 and amendments to Article 4, and in the 2003 proposed amendments, though their victories appear to have been slim.<sup>115</sup> Most of the concerns, however, appear to lie with the failure of the proposed revisions to address issues of interest to consumers not currently addressed by the U.C.C., such as late fees or the unbanked, rather than with the risk allocations that were provided.<sup>116</sup>

With respect to the second claim, it is plausible that the law as applied currently does distinguish between consumer and non-consumer users, notwithstanding formal uniformity in the applicable standard. The formal rules may obfuscate some distinctions that implicitly reflect the occasional differing capacities of consumers and non-consumers to avoid risks. The formal rules make no distinction, for instance, in the standard of care to be used by a consumer or non-consumer drawer. However, some distinction may exist in the application of these formal rules, because what satisfies the standard for a member of one group may vary from what satisfies the standard for another group. For instance, section 3-406 precludes a drawer who fails to exercise ordinary care from asserting a forgery. But what constitutes ordinary care for a consumer may differ from what qualifies for a non-consumer. Employers may be expected to create systems that preclude any one employee from having too much control over the processing of incoming or outgoing checks. Consumers are not expected to add multiple layers of precaution, although they may be expected to ensure that roommates or other persons who are not co-owners do not have easy access to their accounts.<sup>117</sup> The use of flexible standards such as “ordinary care,” therefore, illustrates a capacity to adjust liability to reflect superior risk avoiding ability. Thus, a formally “uniform” standard implicitly recognizes that it may be appropriate to impose liability on non-

114. See, e.g., Kathleen Patchel, *Interest Group Politics, Federalism, and the Uniform Laws Process: Some Lessons from the Uniform Commercial Code*, 78 MINN. L. REV. 83 (1993); Edward Rubin, *Efficiency, Equity and the Proposed Revision of Articles 3 and 4*, 42 ALA. L. REV. 551, 552–57 (1991).

115. See, e.g., Gail K. Hillebrand, *Revised Articles 3 and 4 of the Uniform Commercial Code: A Consumer Perspective*, 42 ALA. L. REV. 679, 682 (1991); Patchel, *supra* note 114, at 86.

116. 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).

117. See, e.g., *Jurcisin v. Fifth Third Bank*, No. 2006-10-078, 2007 WL 1731419, at \*1 (Ohio Ct. App. June 18, 2007).

consumers where similar conduct by consumers would allow them to shift the liability to a bank.

In other circumstances, however, the law with respect to checks creates no distinction between consumers and non-consumers. For instance, both groups are obligated to review items reflected on statements with reasonable promptness after statements are made available and to notify the drawee of any discrepancies.<sup>118</sup> Presumably, relative to the drawee bank, members of each of these groups are in a superior position to detect forgeries and alterations on checks drawn from their accounts. As a result, from a risk allocation perspective, there is little basis for distinguishing between them for purposes of the notice requirement.

Finally, one might advocate bank liability over consumer liability on an insurance rationale. Return to the proposition mentioned above that losses that flow from unauthorized payments, and that are not placed directly on the consumer, must be borne somewhere within the payment system, and that consumers are ultimately likely to bear those losses through the fees they pay for payment services. Financial institutions that bear these costs in the first instance are likely to seek to pass on as many of the costs as possible to customers. The effect is that all consumers will pay for the errors made by any consumer that leads to an unauthorized debit or credit card charge. At least where losses do not result from negligence, this may be an appropriate strategy. It effectively provides each consumer with an insurance policy against conduct that leads to catastrophic loss (or less) from one's credit card or bank account. The small amount by which financial institutions that initially bear the losses will raise fees to any consumer may constitute a premium for providing that insurance. In addition, as we have noted above, financial institutions and card networks are likely in better positions to develop and implement anti-fraud technologies than consumers, so that inducing the former to seize their advantage will likely reduce the total costs related to unauthorized payments and precautionary behavior.

As we implied above, however, the "insurance" justification suggests that the talisman of "consumer protection" should not be taken to absolve all consumers from all losses in all circumstances. Rather, it should be taken as a basis for determining what kind of consumer behavior should be considered. Presumably, consumers as a class would

118. U.C.C. § 4-406(c) (2005).

prefer to insure against risks to which all consumers are relatively equally exposed. If consumers as a class are, with low variance among class members, exposed to risks of theft and forgery, then presumably consumers as a class would be better off with class-based insurance supported through bank fees. But if most members of the consumer class would take a level of care with respect to the risk of unauthorized payments, then it is less clear that the majority would want to subsidize those whose negligence increases losses from unauthorized payments for which all consumers must pay insurance premiums. That is, consumers as a class may prefer not to insure against a level of inadvertence that would be exhibited only by a few.

Indeed, even outside the consumer area, the consequences of system user negligence seem peculiarly non-uniform. In the area of business checks, as in the area of consumer checks, a drawee or depository bank will be able to shift all or part of the loss from fraud on the business system user, depending on the bank's own exercise of ordinary care. Again, comparative negligence principles will apply where both parties failed to exercise ordinary care.

Compare that situation to the result when parties to wholesale wire transfers fail to exercise ordinary care. A bank that executes a payment order will be able to charge its customer the amount of the order, even if the order was unauthorized, if the bank and the customer agreed that the authenticity of payment orders would be verified pursuant to a security procedure and the bank accepted the payment order in good faith and in compliance with the security procedure.<sup>119</sup> The underlying assumption is that if an unauthorized person was able to circumvent the approved security procedure, the customer was presumptively negligent in failing to supervise an employee or in publicizing the information necessary to transmit the payment order to the bank. Thus far, the result is consistent with what would happen if a negligent customer contributed to the making of a forgery on a check.

But what if the bank is also negligent with respect to execution of an unauthorized payment order? That negligence would presumably consist of failure to follow an agreed-to security procedure. For instance, a bank might neglect to employ a required callback procedure or accept a payment order that was sent unencrypted in violation of the procedure. A bank that fails to comply with the terms of the secu-

119. U.C.C. § 4A-202.

rity procedure will be able to shift any part of the loss from executing an unauthorized payment order back to the customer, notwithstanding that the customer was itself negligent. In short, contributory negligence, rather than comparative negligence, principles apply. This result obtains notwithstanding that Article 4A was drafted at approximately the same time that comparative negligence principles were incorporated into the revisions to Article 3. Given that the primary justification for the latter was that comparative negligence represented the most recent jurisprudence with respect to negligence principles, the divergent treatments of bank negligence in Articles 3 and 4A seems even more difficult to justify.

Assuming that parties, especially commercial parties, would prefer default rules that minimize the total costs of fraud and anti-fraud precautions, there seems little reason to believe that the objective would be achieved through comparative negligence principles for checks and contributory negligence for wire transfers. There is some appropriate debate about which of these systems best induces care by parties optimally positioned to take it.<sup>120</sup> But there is no reason to believe that resolution of that debate will be different for different payment systems. This conclusion is consistent with our argument for diversity in payments system rules. The argument is that different parties, or the same parties in different transactions, might prefer to allocate some payment risks differently across payment systems. The risk of an unauthorized use simply is a risk that is optimally allocated between banks and their customers the same way, regardless of whether payment is made by check or wire transfer.

#### *D. Reversibility of Payment*

##### 1. Minimizing the Costs of Defective Transactions

The rules related to reversibility of payments come into play primarily when a user of a payments system is disappointed with a good or service that the user has purchased. Thus, the risk involved is of product quality, a risk that we refer to as a defective transaction. Defective transactions are socially wasteful because they involve the receipt of a good or service that has a lower value than the purchaser

120. See Robert D. Cooter & Edward L. Rubin, *A Theory of Loss Allocation for Consumer Payments*, 66 TEX. L. REV. 63, 75 (1987); Mann, *supra* note 4, at 638-39; Rogers, *supra* note 2, at 467-72.



agreed to pay and require that some party seek redress from the supplier. These costs would be minimized if the loss that resulted from the transaction was incurred either by the party who could best prevent the defective transaction from occurring in the first instance or who could most easily obtain redress after its detection. The law of reversibility can therefore serve these social purposes if it induces the party who occupies that position to take advantage of his or her situation. If, for instance, payment system providers are well positioned, relative to payment system users or to merchants to detect and deter defective transactions, then it makes sense to have a broad rule of reversibility between the buyer and merchant, thus inducing the payment system provider to monitor against defective transactions and to obtain redress when they occur. It is plausible, however, that different parties will occupy the relevant positions. That is, the user of a payment system may be in a superior position to avoid the defective transaction from occurring in the first instance by carefully selecting sellers or by inspecting goods prior to payment. But in an economy in which consumers cannot easily inspect goods until after payment (either because the goods are packaged or are delivered subsequent to payment), it is not always clear that the payment system user is well positioned to avoid the transaction. And once a defective transaction has occurred, it may be that the payment system provider is in the superior position to seek redress. In the face of uncertainty about who is in the best position to minimize the costs of defective transactions, a menu system that allows different parties to select different risk allocation mechanisms may permit the best matching of risks and transactional preferences. Alternatively, a greater degree of uniformity may be desirable if one party to payment transactions systematically occupies the best position to minimize the costs related to defective transactions.

From this perspective, current law seems confused. Initially, purchasers would appear generally to stand in a superior position, relative to their banks, to select merchants who are likely to complete a contract with a conforming good or service or who are likely to provide redress should a transaction go awry, assuming that consumers have access to reputational information concerning their sellers. Thus, at least with respect to sellers who are geographically proximate to their buyers, it seems likely that buyers will be well positioned to avoid defective transactions or to obtain redress when such a transaction materializes. Nevertheless, it is plausible that buyers, especially consumers, may also purchase certain goods so infrequently, or from sellers about whom reputational information is so thin, that the buyers have little

reliable information about their sellers. This may be particularly the case with respect to online transactions with anonymous sellers, notwithstanding the availability of feedback about sellers from other buyers,<sup>121</sup> or with respect to sellers who are geographically distant from their buyers. Those same sellers, however, may be repeat players with respect to payment system providers or payment networks to which those providers belong. In these circumstances, it is possible that the payment system provider could have information or access to information that would either deter defective transactions or that would facilitate recovery on behalf of the buyer. In these latter cases, legal rules that place the risk of defective transactions on the payment system, by permitting the user to reverse payment and thus requiring the provider to recover from the merchant, would appear justifiable.

From this perspective, at least part of current law arguably gets the legal rule backwards. The Truth in Lending Act permits consumers who have charged purchases to assert against their card issuer any defense that they could have asserted against the merchant.<sup>122</sup> The practical effect of the provision is to permit issuing banks to charge back against the merchant any amount previously paid in respect of the contested charge. The merchant then bears the burden of demonstrating that it provided a conforming performance. The consumer buyer has no right to assert claims against the issuer bank, however, if the charge has been incurred in a transaction that takes place outside the consumer's state of residence and more than 100 miles from the consumer's home. Thus, the consumer has greater rights to reverse payment with respect to geographically proximate transactions than long-distance ones. Putting to the side the issue of where a telephonic or online transaction "occurred," this seems inconsistent with the notion that consumers are likely to have superior information and capacity to obtain redress with respect to merchants who are geographically proximate, since consumers are likely to be repeat players with respect to those merchants. Since, in an age where credit card solicitations are nationwide, credit cardholders will not necessarily possess a card issued by a bank located in the same area as the cardholder's residence, there seems to be less reason to believe that the card issuer will have significant information about the merchant.

121. For a discussion of the limitations of online feedback mechanisms, see Clayton P. Gillette, *Reputation and Intermediaries in Electronic Commerce*, 62 LA. L. REV. 1165 (2002).

122. 15 U.S.C. § 1666i(a) (2000). The right expires if the purchaser has paid for the item. See 15 U.S.C. § 1666i(b).

It is possible, of course, that a card network would be able to obtain information about merchants who have been the subject of frequent chargebacks and to monitor their performance, presumably at lower cost than consumers who face higher informational barriers to monitoring. A threat to terminate the merchant from the network could serve as a significant deterrent to merchant misbehavior. On that understanding, issuer banks may stand in a relatively good position to detect and deter defective transactions. But, given that such information will be largely quantitative and may not reflect the nuances of situations, such as the nature of the defect and efforts to resolve the dispute, and may not include information about disputes that were informally resolved, the banks' informational advantage may be most salient in long-distance transactions, rather than those that occur in environments where consumers are likely to be familiar with merchants' reputations. Thus, current credit card law effectively gives consumers the right to assert defenses against card issuers in the only situation where consumers are likely to have better information about merchants than card issuers, and to deny the right in the very cases in which card issuers might be better positioned to avoid the risk of defective transactions than the consumers themselves.

The analysis to this point has assumed that the alleged defective transaction has occurred because of merchant misbehavior and asked who, as between the buyer and the payment system provider, can best detect and deter that misbehavior. There is, however, an alternative explanation for the allegedly defective transaction. It may be that the transaction conforms to the terms of the transaction, but that the consumer seeks to reverse payment either out of regret, a misperception of the good's characteristics, or a calculated effort to exploit sellers.<sup>123</sup> Consumers, for instance, may be serial "returners" of goods that they have used for a limited period of time, a phenomenon that explains why sellers of large screen televisions allegedly suspend their money-back guarantees during Super Bowl season.<sup>124</sup> Alternatively, consum-

123. See, e.g., R.A. Fullerton & G. Punj, *Repercussions of Promoting an Ideology of Consumption: Consumer Misbehavior*, 57 J. BUS. RES. 1239, 1240-41 (2004).

124. See, e.g., Sandra Block, *Stores Toughen Return Policies*, USA TODAY, Dec. 27, 2005, at 3B. Are post-Super Bowl returns really a problem? We don't know of any statistical study of the phenomenon. But some anecdotal evidence indicates that it is a prominent element of the general phenomenon of consumer misbehavior. A recent blogger, commenting on the elimination of a very liberal return policy at Costco, wrote:

I actually work for Costco in Bridgewater, NJ and I have to say that we all saw this policy change coming, we've been saying it for years that it has to change. The problem with this policy is that, while it is used for it's intent of standing behind merchandise by some, it is also highly abused by many others. In my store, I've worked in the refunds

ers may seek to return goods as defective when consumers are responsible for the defective nature of the good.<sup>125</sup> We group those motivations as “consumer misconduct.” If we believed that most allegedly defective transactions were attributable to consumer misconduct, then there would be little reason to facilitate reversibility of payments. Where consumer misconduct or misuse is observable to sellers, but not verifiable, merchants may justifiably refuse to accept returns. Payment system providers, however, may be in a relatively good position to detect consumer misbehavior, insofar as they can discern patterns of serial returns or protests by the same consumer who deals with different merchants.<sup>126</sup>

Rules with respect to reversibility, therefore, might be adjusted to take better advantage of the relative capacities of merchants, buyers, and payment system providers. But if informational advantage is what justifies reversibility in any case, it is even less clear that the differences in reversibility rules make sense. The credit card rules bear no relationship to rules in other systems. The law with respect to debit cards contains no provision for reversing a transaction, regardless of whether the transaction is processed in a manner that makes debits from the cardholder’s account essentially simultaneous with the transaction, or whether the transaction is processed through a slower network with signatures and paper receipts akin to credit card transaction processing. Check transactions permit the drawer to coun-

department, so I’ve seen this first hand. We have one particular member (We all know him by name, but I won’t post it here out of courtsey [sic]) who will buy TVs, cameras, Ipods, etc and return them every time a new model comes out. Now, aside from use, there[’]s nothing wrong with the items he returns, he just wants newer models. He’s not the only one to do this, there are more. Just this past summer, we accepted a refund on a laptop from a different member. The laptop was 4 days shy of 6 months old (the limit on laptop refunds). When we looked further into this account, it turns out that, in the span of 2 years, this particular member purchased 13 laptops and desktops and returned all but 2 of them. This is clear abuse of a generous policy. We see similar returns seasonally. In the summer, we have an influx of shovels and snow throwers returned. In the winter/fall, we get back patio furniture, grills, lawn mowers, etc. We also get a mad rush of Post-Super Bowl TV refunds. People use our policy as a way to “rent” items, not as a promise to stand behind faulty merchandise. It’s a shame that some people feel no guilt in doing this. Not only do they ruin the policy for others, but in doing so, they are also driving up costs of all other merchandise.

Posting of A Costco Employee (Mar. 19, 2007, 12:48 EST) to Blueprint for Financial Prosperity, <http://www.bargaineering.com/articles/> (Mar. 1, 2007).

125. See, e.g., *Izraelewitz v. Mfr. Hanover Trust Co.*, 465 N.Y.S.2d 486, 487–89 (N.Y. Civ. Ct. 1983); *Bartus v. Riccardi*, 4 UCC Rptr. Serv. 845, 846 (N.Y. Civ. Ct. 1967).

126. We agree with Ronald Mann that it would be useful to know the frequency with which cardholder claims prevail. See Mann, *supra* note 4, at 660. But rates with which the claims prevail may not be the same as rates with which merchants or consumers misbehave. As Mann indicates, merchants may agree to give credits to avoid further difficulties with credit card issuers. Consumers may abandon valid claims because they cannot afford to litigate them.

term and the order by issuing a stop payment order. The drawee bank is obligated to comply with the stop payment order, as long as it receives the order in time to act on it before it makes final payment of the item. While electronic presentment and remote deposit capture reduce the relevant time period, it is still plausible that the period between check delivery and presentment will be sufficient to allow consumers to inspect the quality of goods and act on dissatisfaction. Where a stop payment order is otherwise effective, no investigation into the alleged defects in the underlying transaction is either necessary or appropriate. Moreover, a drawee bank that improperly makes payment over a stop payment order is subrogated to the rights of the payee or a holder in due course of the item. As a result, a drawer who issues a timely stop payment order in a transaction that is not, in fact, defective will be able to require the payee to seek payment for the goods or services provided. But a bank that pays over the stop payment order will be able to enforce the check against the drawer.

These rules may make some sense from the perspective of protecting the finality of transactions. Credit card transactions are arguably not final until the issuer has billed the card holder and received payment with respect to the transaction. Thus, allowing the transaction to be undone does not require unwinding a completed transaction. The same cannot be said about debit cards, at least in theory, since withdrawal of the payment amount from the card holder's account is expected to be simultaneous with the transaction. In practice, there may be substantial departures from theory, especially with respect to signature-based cards that are processed along paper networks. In those cases, prompt efforts at reversing the transaction could provide notice to the card issuer prior to the time that the card holder's account is debited. But, as in the case of the expanded definition of electronic fund transfers to cover all debit card transactions,<sup>127</sup> there may be some value to treating all debit card transactions identically to avoid consumer confusion. Finally, check rules tie reversibility explicitly to the finality of the transaction. Again, a stop payment order is effective as long as it is received prior to the point that is basically equivalent to final payment.<sup>128</sup>

But why should finality matter? Certainly there are costs to unwinding a completed transaction. Expectations have been settled; merchants may have restocked inventory or assumed additional

127. See *supra* note 64 and accompanying text.

128. See U.C.C. §§ 4-215, 4-303 (2005).

obligations based on completed transactions. But in a mass market economy, we question whether the number of transactions that need to be undone will dramatically affect merchant behavior, and the costs of reversing transactions must be weighed against the losses that can be avoided if defective transactions are deterred by reversibility or if merchants are better positioned to minimize the costs related to defective transactions, for instance by reselling the goods. Moreover, the merchant who accepts a credit card in payment is unlikely to forestall restocking inventory or forgo alternative transactions out of concern that a "completed" credit transaction will be undone. In short, finality seems to be less of a factor relevant to the proper allocation of defective transactions costs than the issue of superior loss avoiding or loss bearing.

It is less clear that the analysis we provided above with respect to minimizing defective transactions applies with equal force outside the credit card setting. The closest case would appear to be the debit card, since the same or similar networks that provide credit card processing exist in the debit card environment. Thus, the ability to monitor buyers and merchants, to reverse credits and debits, and to deter defective transactions in the first instance favors similar degrees of reversibility, assuming that the costs of undoing the "finalized" transaction are not too high.

The case of checks is more difficult. Drawee banks may be able to monitor customers who issue high levels of stop payment orders, and who therefore appear to be engaged in consumer misconduct. But given that drawee banks face no liability for dishonoring checks subject to a stop payment order,<sup>129</sup> they have little incentive to take advantage of this position. Moreover, drawee banks will have little information about payee merchants similar to the information that might be available through their membership in card networks. While they may be able to obtain information about merchant payees where those merchants are also members of the card networks to which the drawee bank belongs, the drawee will not have an easy mechanism for reversing credits given through the check collection system. Thus, initially we might think that there is little reason to provide reversibility in the check context similar to the capacity of credit card users to assert against card issuers the defenses that the card holders have against merchants.

129. *See id.* § 3-408.

But that conclusion may be too facile, for two reasons. First, there is nothing technologically impossible about allowing credits due to checks to be reversed after final payment. Indeed, that is exactly what we would expect to happen in the event of payment of a check in violation of a transfer warranty or presentment warranty. Second, in the event that the merchant payee is also a member of a card network to which the drawee bank belongs, we could imagine a process by which the bank could undo a check payment by reversing credits given through the credit card system. There is no *a priori* reason to seal each payment system hermetically from every other system. The issue again is whether payment system providers stand in such a superior position to deter and resolve defective transactions that we would want to place on them the legal obligation to take advantage of that position. If so, then more uniformity in rules that place the burden on payment system providers would be appropriate; if not, then not. That is an empirical issue that we cannot decide. But we believe that it is a more relevant factor in the reversibility debate than the traditional appeal to finality.

## 2. Billing Errors and Reversibility

Current law on defenses against card issuers makes even less sense when considered with rules on billing errors. Assume that a cardholder does not receive goods prepaid with a credit card and pays the related charge in full, perhaps because the time for delivery has not yet expired. Several months later, after expiration of the time for delivery, the cardholder seeks to set off the amount of the charge with respect to the undelivered goods against subsequent charges on the cardholder's card. One might think the cardholder is precluded from shifting the burden of redress to the card issuer. The provision that allows the cardholder to assert defenses arising from the underlying transaction against the card issuer applies only to the extent of "credit outstanding with respect to such transaction" when the cardholder gives notice of the defective transaction to the card issuer.<sup>130</sup> This provision itself may not make sense from the perspective of superior risk bearing, since if the card issuer does occupy the best position to seek redress or to deter the initial misconduct, that position does not appear to be altered by the receipt of payment with respect to the transaction. Nevertheless, the law seems clear on the point. But a different

130. 15 U.S.C. § 1666i(b) (2000).

result is reached if the case is treated as one of non-delivery rather than as a defective transaction. In that case, inclusion of the charge is considered a billing error.<sup>131</sup> With respect to billing errors, a cardholder who gives notice to the card issuer within sixty days after transmission of the statement that references the transaction will not be responsible for ultimate payment of the disputed sum, and is presumably entitled to a credit from the card issuer if that payment has already been made.<sup>132</sup>

The inconsistency in treatment is exacerbated by judicial decisions that have also negated the consequences for consumers of failure to comply with the sixty-day requirement for giving notice to the card issuer. Courts have held that a cardholder retains defenses to payment against the issuer even when the consumer fails to give timely notice in accordance with 15 U.S.C. § 1666(a).<sup>133</sup> Thus, the cardholder's failure to notify the issuer does not deprive it of the right to have its account credited in the amount of the related charge. From the perspective of efficient precaution-taking, this gets the wrong result. The card issuer is in an inferior position to take cost-justified precautions against the initial use of the credit card to an untrustworthy merchant. Even if one were to argue that the card issuer could have deterred the initial transaction by monitoring poorly performing merchants, the calculus of precaution costs change when the cardholder receives its credit card bill. At that point the cardholder can detect a charge with respect to undelivered goods at less cost than the issuer must invest to discover the seller's noncompliance. The cardholder simply needs to read his or her statement and inform the issuer. Once informed, any asymmetry in information between the issuer and cardholder with respect to authorization is eliminated. The Truth in Lending Act's "billing error" rule, by giving the cardholder sixty days in which to give notice to the issuer, saves the cardholder what might otherwise be burdensome costs of discovering improper charges immediately. But if that burden is sufficiently reduced by the grant of a sixty-day discovery period, then a rule that allows a cardholder to assert defenses to payment based on non-delivery, notwithstanding the failure to give the issuer

131. *Id.* § 1666(b)(3).

132. *Id.* § 1666(a).

133. *See, e.g.,* Citibank (S.D.), N.A. v. Mincks, 135 S.W.3d 545, 558 (Mo. Ct. App. 2004); *see also* Dillard Dep't Stores, Inc. v. Owens, 951 S.W.2d 915 (Tex. Ct. App. 1997) (finding that plaintiff complied with sixty-day limit and defendant failed to provide an appropriate written explanation as to why it refused to refund the erroneous charges).



notice, shifts non-recoverable losses away from the cardholder who occupies a superior position to detect the loss.

There may be cases in which the sixty-day period is insufficient to trigger cardholder action. Assume, for instance, that the cardholder orders goods that must be prepaid, but that will reasonably take more than sixty days to manufacture and send to the cardholder. The prepayment requirement means that the charge will show up on the cardholder's statement immediately. The manufacturing requirement means that the cardholder will not know of the non-delivery until a period more than sixty days after receiving the statement that contains the related charge. In such a case, there is little reason to believe that the cardholder was better positioned to detect nonperformance or to seek redress. Indeed, if the subsequent non-delivery is precipitated by the seller's actual or impending failure, the card issuer is likely in a superior position to detect the loss, because the complaining cardholder is unlikely to have been the only one victimized by non-delivery. Nevertheless, the rule is not written in a manner that restricts the shift in liability to cases that fit those circumstances.

#### *E. Preclusion Rules as Default Terms*

The case for diversity in payment systems rules has an implication for the alterability of these rules. Parties to transactions might prefer to allocate risks in a manner that is not reflected in any of the state-supplied payment rules that could apply to their transaction, either because the level of risk aversion varies from that assumed by the state-supplied rule or because the details of their transaction idiosyncratically cause a party not typically well positioned to avoid risks to be able to do so. The argument that payment rules should be considered as means of risk management thus also suggests that the provisions should be default rules.<sup>134</sup>

134. The distinction between default and mandatory payment rules is not absolute. The difference is one of degree only. Payment rules are applicable to contracts calling for particular forms of payment. As often noted, in a sense all rules governing contracts are default terms because parties can avoid the application of any rule to their agreement at greater or less cost. If an explicit and clear statement is needed to opt out of a rule, the parties' agreement can include the required statement. A choice of law clause can select a jurisdiction's law that enforces terms provided by the agreement. In the limit, arbitration clauses can assure the selection of a law or a decision maker who will enforce terms provided in the agreement. Default terms matter when parties have a bias in favor of terms supplied by background law or when they are asymmetrically informed about matters bearing on their agreement. See Ian Ayers, *Menu Matter*, 73 U. CHI. L. REV. 3 (2006); Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203, 1205–06 (2003). Otherwise, default and mandatory terms are distinguishable only by the parties' cost in contracting for the terms they prefer.

Although most of payments law consists of default rules, the extent to which its specific rules are alterable by contract differs across payment systems. Article 4, 4A and 5's respective general provisions governing alteration, for instance, are more or less permissive. With few exceptions, they allow parties to vary their provisions, subject to requirements of good faith and reasonable care.<sup>135</sup> Even standards of good faith or ordinary care can be supplied by agreement, if not "manifestly unreasonable."<sup>136</sup>

The alterability of specific rules governing claims of payment system users against payment providers, however, differs between checks and wholesale wire transfers. For checks, 4-406(f) places a one-year outer limit from the date a bank statement is made available to the customer in which the customer must report forgeries or unauthorized alterations. A customer failing to meet this deadline has no claim against its bank.<sup>137</sup> This rule precludes the customer from recovering from the bank, even if the claim is asserted within Article 4's three-year statute of limitations.<sup>138</sup> Section 4-406(f) does not prevent a bank and its customer from reducing the limitation period by contract, and courts generally uphold "cutdown" clauses drastically shortening 4-406(f)'s one-year outer limit.<sup>139</sup> Cutdown clauses that apply without regard to the bank's good faith or ordinary care apparently also are enforceable.<sup>140</sup> Little distinction appears to exist between consumer and non-consumer customers for these purposes.

The little law on the preclusion rule for wholesale wire transfers considers it a mandatory rule. Under 4A-505, a customer who has paid its receiving bank that has executed a payment order has no claim for a refund unless the customer notifies the bank within one year after the bank has notified the customer of the payment order. Section 4A-501(a) allows the parties to a funds transfer to vary the terms of their

135. *See, e.g.*, U.C.C. §§ 4-103(a), 4A-501(a), 5-103(c) (2005). Institutional rules made applicable to a letter of credit by contract or usage can be varied. *See, e.g.*, INT'L CHAMBER OF COMMERCE, ICC UNIFORM CUSTOMS AND PRACTICE FOR DOCUMENTARY CREDITS art. 1 (2006).

136. U.C.C. § 1-102(3) (1962); U.C.C. § 4-103(a) (2005).

137. U.C.C. § 4-406(f) (2005).

138. *Id.* § 4-111.

139. *See, e.g.*, *Stowell v. Cloquet Co-op Credit Union*, 557 N.W.2d 567, 571-72 (Minn. 1997) (twenty days); *Nat'l Title Ins. Corp. Agency v. First Union Nat'l Bank*, 559 S.E.2d 668, 671 (Va. 2002) (sixty days); *Borowski v. Firststar Bank Milwaukee, NA*, 579 N.W.2d 247, 252-53 (Wis. Ct. App. 1988) (fourteen days).

140. *Cf. Pinigis v. Regions Bank*, No. 1060474, 2007 WL 1953895, at \*10 (Ala. July 6, 2007); *Halifax Corp. v. First Union Nat'l Bank*, 546 S.E.2d 696, 703 (Va. 2001) (bank's bad faith does not extend one-year limit); *Nat'l Title Ins. Corp.*, 559 S.E.2d at 671 (relying on *Halifax* to enforce cut-down clause).

funds transfer agreement, “[e]xcept as otherwise provided in this Article,” and 4A-505 does not explicitly prohibit the parties from altering this one-year limit by agreement. Because a number of provisions in Article 4A are made mandatory by their terms,<sup>141</sup> a fair inference from 4A-505’s silence on the matter is that its one-year limit can be varied by agreement. But in *Regatos v. North Fork Bank*,<sup>142</sup> the New York Court of Appeals disagreed. While finding the question close, the court concluded that 4A-505’s one-year limit is a mandatory rule: allowing customers and their banks to agree to a different limit would alter Article 4A’s “fine-tuned balance” between them.<sup>143</sup> Payments law therefore adopts different preclusion rules for checks and wire transfers.

The law on the alterability of preclusion rules for checks and wire transfers is mistaken. In fact, as with reversibility rules, it is arguable that the proper status of the rules is at least partially backwards from current doctrine. The case for diverse payments rules made above suggests that the variability of the preclusion rule should be different for firms and for consumers, and that the preclusion rule for consumer checks should be a mandatory rule, while the preclusion rule for business checks and wire transfers should be a default rule. Section 4-406(f)’s preclusion rule purports to induce prompt investigation of statements to discover unauthorized signatures and alterations. Once the bank has notified the customer about debits to its account, the customer has the information needed to detect forged or unauthorized alterations to checks.<sup>144</sup> At that point the customer is better positioned than the bank to prevent ongoing forgeries or alterations by the same wrongdoer. It need only examine statements and notify the bank of any discrepancies. Once notified, the bank is in a better position than the drawer to prevent further forgeries or unauthorized alterations, or to recover unauthorized payments.

Section 4-406(f)’s preclusion rule dictates to the bank the period of time in which it must preserve evidence about notification dates,

141. See, e.g., U.C.C. §§ 4A-202, 4A-203, 4A-305 (limiting alteration of rules governing security procedures, limiting alteration of specific rules governing security procedures, and allowing recoverable consequential damages only when provided for by express written agreement, respectively).

142. 838 N.E.2d 629, 633 (N.Y. 2005).

143. *Id.* at 633. Unsurprisingly, an informal survey of Article 4A’s committee conducted by the Co-Reporter for Article 4A (William Warren) reveals no agreement on the matter. See WILLIAM D. WARREN & STEVEN D. WALT, *TEACHER’S MANUAL: COMMERCIAL LAW* 366–67 (7th ed. 2007). *Steffes v. Heritage Bank NA Willmar*, 48 UCC Rep. Serv. 2d 287, 290–91 (Minn. Ct. App. 2002), interprets U.C.C. section 4A-505 as a default rule.

144. See *Am. Airlines Employees Fed. Credit Union v. Martin*, 29 S.W.3d 86, 92 (Tex. 2000).

finance litigation reserves for defending against claims for unauthorized payment, and finance loss reserves resulting from unauthorized payments. Cutdown clauses reduce these costs and therefore should lower the price banks charge to maintain deposit accounts. But, even if those savings are passed onto customers, the savings are worthwhile only to the customer who does not incur a higher expected loss by virtue of being unable to recover from the drawee for unauthorized debits discovered after the cutdown period. In short, customers will benefit from a fully-priced cutdown period only if they are in a position to calculate whether the resulting savings in banking services costs exceed the value of their greater exposure to undetected fraud. Consumers, however, may systematically underestimate the consequences of agreeing to a cutdown clause, and thus underprice the clause, because at the time they agree to it they will have little information concerning its expected value. Nor are banks likely to compete over the time periods that apply under section 4-406(f) in ways that make different clauses salient to consumers. As a result, consumers may be led to select terms they do not prefer. For both reasons, consumers may be better off with a single preclusion rule like section 4-406(f). This arguably justifies making section 4-406(f) a mandatory rule for consumer users of checks.

One might contend that differential preclusion periods are unnecessary, because non-consumer customers who have better information about fraud risks can serve as effective proxies for consumers, since section 4-406(f) and the cutdown clauses will nominally apply to both. It is not clear, however, that the interests of consumers and non-consumers are sufficiently aligned to confirm the proxy argument. Non-consumers may be more susceptible to fraud, since a great deal of check fraud involves misfeasance by employees. In addition, non-consumers are likely to be dealing with checks written in greater amounts than consumers. The combination of higher rates of check fraud and higher losses per case means that non-consumers face a higher expected loss from check fraud than consumers. As a result, non-consumers have incentives to discover fraud quickly. Non-consumers are therefore more likely to agree to a cutdown clause, since they will have less need for the full statutory period in any event. If that is the case, then non-consumers would not be suitable proxies for consumers, who might have less incentive to examine statements promptly. In short, while non-consumers may have better information than consumers about whether pricing of banking services with a cutdown clause makes a reduction of the statutory period worthwhile,

non-consumer calculations of the tradeoff do not necessarily reflect the same risk/benefit calculus that consumers face. Thus, non-consumer calculations cannot compensate for the informational deficiencies that consumers suffer. While access to information may justify contractual variations from the statutory period in the case of non-consumers, that is less likely to be the case for consumers. Nor can we rely on market competition to fill the informational void for consumers. Given the low probability of check fraud for consumers, neither the statutory default rule nor the contractual cutdown period is likely to be salient to consumers at the time they open accounts. A consumer is likely to become aware of the notification requirement only after fraud in his or her account materializes. Banks, therefore, are unlikely to compete for customers by avoiding cutdown periods or offering pricing tradeoffs for them.

If we are correct about the distinctions between consumers and non-consumers, then there might be reason to bar cutdown clauses in the case of consumers. The proposal to bar such clauses in the case of consumers is limited by the strong behavioral assumptions needed to support it. Consumer users of checks may not be subject to the cognitive failures identified in sufficient numbers to warrant barring cutdown clauses. Even if prevalent, the trouble might be remedied by detailed disclosure or statutorily mandated forms of “cognitive therapy” without refusing to enforce them. The behavioral research on the effects of over-optimism and complexity on choice may not be robust enough to easily apply to consumer users of checks.<sup>145</sup> Thus, under limited conditions, a statutory preclusion rule justifiably may be made mandatory.<sup>146</sup>

But even if there is a limited case for imposing mandatory preclusion rules for consumers, there is much less reason to deprive parties

145. Compare Colin F. Camerer & Dan Lovallo, *Overconfidence and Excess Entry*, in CHOICES, VALUES, AND FRAMES 414–23 (Daniel Kahneman & Amos Tversky eds., 2000) (overconfidence among experimental subjects resulting from extrapolation of current trends), with David A. Armor & Shelly E. Taylor, *When Predictions Fail: The Dilemma of Unrealistic Optimism*, in HEURISTICS AND BIASES: THE PSYCHOLOGY OF INTUITIVE JUDGMENT 334–47 (Thomas Gilovich, Dale Griffin & Daniel Kahneman eds., 2002) (questioning extent of optimism in predictions), Sheena S. Iyengar & Mark R. Lepper, *When Choice is Demotivating: Can One Desire Too Much of a Good Thing?*, 79 J. PERS. & SOC. PSYCH. 995, 1003 (2000) (people respond to increasing number of options by relying on simple rules to make choices), and Jeffrey J. Rachlinski, *Gains, Losses, and the Psychology of Litigation*, 70 S. CAL. L. REV. 113 (1996) (summarizing literature finding that structure of choice produces suboptimal decisions).

146. We recognize that some states have modified the official version of section 4-406(f) to provide a statutory cutdown period. See, e.g., GA. CODE ANN. § 11-4-406(f) (West 2002) (sixty-day period for reporting unauthorized signature or alteration).

to wholesale wire transfers from treating the state-supplied preclusion as only a default. A customer and its bank making the funds transfer may have different risk-bearing capacities than most customers and banks. In such cases the bank will offer to execute a wire transfer at a lower price if section 4A-505's one-year limit is reduced than if the wire transfer remains subject to it. The customer will prefer the lower priced contract if the increased risk placed on it under the contract is less than the reduction in price. Absent in wholesale wire transfers are informational asymmetries, effects on third parties, or paternalist concerns that warrant a mandatory rule. Wholesale wire transfers occur between non-consumer originators and banks, and often between repeat players, so that neither party systematically lacks relevant information more than in any other sort of contract between commercial parties. Unlike the consumer customer, the non-consumer originator of a wire transfer easily can learn about the reputation and abilities of its receiving bank. It does not benefit from signals that mandatory terms might provide about the bank's trustworthiness or competence. Because the costs of negotiating, performing, and enforcing wholesale wire transfers presumably are impounded in the price of wire transfer, non-pecuniary externalities aren't present. Paternalism also is not a concern because the parties are non-consumers. The originator therefore does not require protection. Even if non-consumer originators required protection, no normatively-compelling principle describes the way in which they ought to be protected.

Article 4A's drafting involved extensive negotiations, principally between representatives of banks and corporate and commercial users of funds transfers.<sup>147</sup> The bargaining produced a set of rules that presumptively reflect the preferences of the majority of banks and corporate and commercial users. For a minority of banks, the costs of maintaining large reserves to refund payments and the potential loss from being unable to recover mistaken or unauthorized payment orders downstream during section 4A-505's one-year limit may be too high. Correspondingly, their originators might be able to take cost-justified precautions in reporting mistaken or unauthorized debit from their accounts sooner than a year after receiving the bank's notice of the debit. The average value of a wire transfer is large, with a wide

<sup>147</sup> Carlyle C. Ring, Jr., *The UCC Process—Consensus and Balance*, 28 LOY. L.A. L. REV. 287, 294–95 (1994).

variance,<sup>148</sup> making an originator's early reporting presumptively cost-justified for some funds transfers. These originators therefore might accept a reduced price for the funds transfer in exchange for a shortened period in which they must report an unauthorized payment. The funds transfer laws of other countries, which allow parties to set a reporting period by contract, enforces such agreements.<sup>149</sup> Section 4A-505 is not by its terms a mandatory rule, and allowing parties to vary its one-year limit effectuates the atypical preferences of a minority of originators and banks. The case for diversity in payments law recommends that Article 4A's preclusion rule be a default rule, like section 4-406(f)'s preclusion rule for checks. The *Regatos* court is mistaken that Article 4A's preclusion rule "fine tunes" the balance between the originator and its bank; the parties' contract instead does this.

#### CONCLUSION

Current law assigns different payment risks differently across some payment systems. Whether this diversity in legal rules is justified depends on whether different payment system rules should be uniform. At a very general level, the standard for selecting rules is the same: the rules that most parties would prefer to govern the payment aspect of their transactions should apply. Most parties usually prefer to minimize the costs associated with a payment term for their transaction. This "meta-principle" therefore usually selects rules which assign the relevant risk of loss associated with a payment term to the party in the superior position to avoid it. However, different parties can be in a superior position to avoid a loss, depending on the type of loss and incentive effects of assigning a risk of loss. Further, where parties are risk-averse or unreliable at evaluating risk, most parties might prefer to shift risk away from these parties, even if they are in a superior position to avoid it. For both reasons, the "meta-principle" need not select the same rules for unauthorized payment, finality, or reversibility of payment, for example, across payment systems. The uniform principle justifies diverse rules for payment systems. The extent of diversity among them turns on a detailed assessment of the comparative risk-

148. See Bd. of Governors of the Fed. Reserve Sys., *Fedwire Funds Transfer System: Assessment of Compliance with the Core Principles for Systematically Important Payment Systems* 9 (2006), <http://www.federalreserve.gov/paymentsystems/coreprinciples/default.htm> (reporting that the median amount of 2005 Fedwire funds transfers was about \$32,000, the average amount was 3.9 million dollars, and about 10% of funds transfers were for more than one million dollars).

149. See, e.g., *GEVA*, *supra* note 1, at 418 (Swiss law).

reducing abilities of parties, as well as attitudes toward risk of users of different payment systems.

This conclusion is not surprising. It resembles the consensus reached in the law and economics literature on the choice of optimal remedy for breach of contract. The literature shows that there is no single optimal remedy when all relevant variables are taken into account. Available remedies result from a variety of variables, ranging from the choice of contracting partner, investment in the contract, the extent of negotiations of contract terms, the care with which the contract is performed, and negotiations in the event of breach.<sup>150</sup> For instance, remedies that encourage efficient breach also can encourage overinvestment in the contract, while remedies that discourage overinvestment can encourage inefficient breach. No single remedy optimally reduces the costs of negotiating, performing, and enforcing a contract. The optimal remedy instead is likely to be some hybrid form of relief.

This Article argues that a similar result holds for rules governing payment systems. Factors bearing on precautions and attitudes toward risk make it unlikely that optimal rules will allocate loss between payment providers and users the same way across payment systems. Informational asymmetries may put one party in a superior position to avoid an element of loss at one time, while another party may be better positioned to avoid it at a later time. Further, a party may be in a better position to pursue risk-reducing technologies at a later time while at present that same party is in an inferior position to avoid loss. The payment system provider or user may be better positioned depending on the type of loss and the payments system. A credit card issuer might be better positioned to detect all unauthorized use of a credit card than its consumer cardholder (statutory assumptions aside), while a drawee bank processing checks under a positive pay program is in an inferior position to its drawer to detect forged checks. This makes it unlikely that the optimal rule for unauthorized use will be the same for credit cards and checks. Again, the card issuer may know more than the cardholder about the likelihood of defective performance by a merchant in the underlying transaction; the card issuer may also have greater leverage over the merchant than the consumer cardholder. The drawee bank or bank executing a wire transfer may not have similar

150. See, e.g., Richard Craswell, *Against Fuller and Perdue*, 67 U. CHI. L. REV. 99, 107–11 (2000); Eric A. Posner, *Economic Analysis of Contract Law After Three Decades: Success or Failure?*, 112 YALE L. J. 829, 834–39 (2003).



advantages in their knowledge of the underlying transaction. Optimal reversibility rules probably will differ between checks and wire transfers. In addition, many users of particular payment systems may be risk-averse or unable to reliably assess relevant risk, so that they prefer to allocate risk of loss without regard to their ability to take precautions. For these reasons, optimal rules for allocating relevant loss will be diverse across payment systems.