UNAUTHORIZED PAYMENT TRANSACTIONS AND WHO SHOULD BEAR THE LOSSES

FRANCIS J. FACCIOLO*

INTRODUCTION

This article is concerned with how losses should be allocated between account holders that are implicated in payment systems and the financial institutions that participate in those payment systems by acting as intermediaries between account holders. It does not consider how losses should be allocated among the various financial institutions. (It is, of course, possible that a financial institution may be the account holder.) Although such an approach is often seen as one focusing on the concerns of individual consumers, the account holders that are discussed in this article are not limited to individual consumers. At times, of course, the nature of the account holder is relevant and, at those points, this article will distinguish between the types of account holders. When a distinction is important, this article will refer to individual and small business account holders as "small account holders."

This article examines how an unauthorized transaction can be prevented and what this suggests about who should bear the loss of such a transaction. In doing so, this article looks at two moments at which an unauthorized payment transaction might be prevented: before the first unauthorized transaction, and after the first unauthorized transaction. An authorized transaction, of course, can be converted, while it is being executed, to an unauthorized one. The classic example is the check that is stolen after it is completed by the account holder by some third party who alters the payee or amount payable. But this article will focus only on the period before the first unauthorized transaction is executed and the period after it is executed.

* Francis J. Facciolo is on the faculty of the St. John's University School of Law. A version of this article was delivered at the symposium on Rethinking Payments Law, April 27, 2007, sponsored by the Federal Reserve Bank of New York. I wish to thank Dean Mary C. Daly for a summer research grant to support my work on this article. In addition, I wish to thank William H. Manz, Senior Research Librarian, and the staff of the St. John's University School of Law library for their invaluable research help.

As many commentators have pointed out, the rules involving payment systems show a wide range of divergent approaches. In the period before a transaction is executed, some payment systems take the possible negligence of an account holder into account in allocating losses for unauthorized payment transactions. The checking system is the classic case.[1] In contrast, the Truth-in-Lending Act (TILA) and the Electronic Fund Transfer Act (EFTA) both ignore the negligence of an account holder prior to the unauthorized transaction.[2]

Article 4A of the Uniform Commercial Code, dealing with wire transfers, adopts a third approach. It includes a strict liability standard for the account holder if the receiving bank has created a commercially reasonable security procedure pursuant to which the transaction is executed.

Professor Gillette focused on the discrepancy between Articles 3 and 4 on the one hand, and the TILA and the EFTA on the other, and concluded that, based on this discrepancy, "[t]he law of payments, therefore, contains a puzzle. Why should regulations that govern functionally equivalent payment devices—checks and cards—vary in both form and substance?"[3] He analyzed three possible explanations: a public choice explanation, a historical explanation, and a third explanation that "identifies discrete differences in the characteristics of checks and cards, and examines whether those characteristics justify the differences in the form and substance of legal regulation."[4] Professor Gillette's conclusion was that "[e]ach of the proffered explanations—public choice, inertia, and selection of an optimal degree of precision—fails to provide a complete understanding of how the current system evolved."[5]

This article asks a question that is implied in Professor Gillette's earlier article but that is not directly addressed or answered. Given the discrepancy between the negligence concepts embedded in the checking system, the rejection of these concepts in the TILA and the EFTA (at least

1. Professor Rogers has distinguished between two types of unauthorized payment transaction: unavoidable and avoidable losses. James Steven Rogers, *The Basic Principle of Loss Allocation for Unauthorized Checks,* 39 WAKE FOREST L. REV. 453, 454–55 (2004). His discussion also includes the situation of a forged indorsement on a check, *id.* at 457–58, which is not discussed in this article. Professor Rogers would disagree with the statement in the main text, at least as it applies to unavoidable losses. *See id.* at 467 ("Thus, the rules on forged indorsements and the rules on forged drawers' signatures together embody a very basic but important principle: *The burden of unpreventable losses should rest with the providers of the payment system rather than with the users of the payment system*.").

2. Robert D. Cooter & Edward L. Rubin, *A Theory of Loss Allocation for Consumer Payments*, 66 TEX. L. REV. 63, 64–65 (1987).

3. Clayton P. Gillette, *Rules, Standards, and Precautions in Payment Systems*, 82 VA. L. REV. 181, 184 (1996).

4. *Id.* at 187–88.

5. *Id.* at 230.

in the pre-unauthorized payment transaction context), and the strict liability approach of Article 4A, should we be considering the adoption of one of these approaches for all payment systems?

Subsequent to the unauthorized transaction, most payment systems (other than credit cards) rely upon the account holder reporting the unauthorized transaction to the financial institution at which the account is held. If the account holder acts promptly, the loss from the first and subsequent unauthorized transactions falls, either by operation of law or contract, upon the other system participants. Who bears the final loss as between these participants is also governed by a web of statutory and contract provisions. If the account holder delays, various levels of loss, depending upon the amount of delay, the type of loss, and the particular payment system, are allocated to the account holder. Finally, all payment systems in which small account holders normally participate (other than credit cards) have some version of a statement rule that either limits or cuts off any recovery of unauthorized losses after some extended period of time. And even the credit card system is beginning to acquire a version of the statement rule through case law.

As prior commentators on unauthorized payment transactions have thought about allocation of losses for unauthorized transactions, they have always come back to the concept that any loss-allocation rule should provide incentives to the party best able to prevent the unauthorized payment transaction at the lowest cost. "Where multiple parties (i.e., either customers or financial institutions) could take such precautions [against loss], regulations should, therefore, place the obligation on the party who can avoid the loss at the lowest cost."[6]

Professors Cooter and Rubin answer, based on the application of the three economic principles of loss spreading, loss reduction, and loss imposition, that "[w]hen an invalid instrument is paid . . . the principles favor strict liability for the financial institution if it alone can reduce the loss. But if both parties can take precaution, and thus reduce the loss, the principles suggest strict and divided liability, with a relatively low limit on the consumer portion."[7] By "strict," Professors Cooter and Rubin meant that there should be no place for negligence principles in allocating losses. In their view, "the great majority of payment losses" should be strictly allocated between both consumers and financial institutions, not solely to financial institutions—an approach that they labeled "complex."[8]

6. *Id.* at 184.
7. Cooter & Rubin, *supra* note 2, at 124.
8. *Id.* at 85.

Professor Mann, writing almost two decades after Professors Cooter and Rubin and almost one decade after Professor Gillette, has suggested that who bears the risk of unauthorized transactions "often should be resolved based on the nature of the underlying technology."[9] In Professor Mann's view, losses are in fact imposed "almost complete[ly]" on system operators because of "an implicit premise that losses in technology-driven systems are most effectively reduced by technological and system-design initiatives that are exclusively within the control of the system operator."[10] He still saw a need to motivate the account holder to take precautions:

> The premise of those rules [allocating losses to system operators] is that even a complete allocation of loss to the network operator will leave the consumer a sufficient incentive to attend to contract provisions that resolve the legal questions summarized above. That could be true because of the hassle of reversing unauthorized charges, because of doubts that financial institutions readily will fulfill their obligations in such a situation, or even because of ignorance of the legal protections for unauthorized transactions.[11]

While Professor Mann's overall summary is true as to unauthorized transactions that could not be prevented by an account holder's due diligence in examining statements (with the notable exceptions of checks, presumably not one of the modern payment systems he is discussing, and Article 4A wire transfers), it is not true of unauthorized transactions that could be prevented by an account holder's paying attention to her account and its associated statements.

In addition, the different rules underlying checks and credit cards have allowed the courts to engage in some creative lawyering. Negligence has begun to migrate from the bank statement rule in Article 4 of the U.C.C. to the TILA, particularly in the Second Circuit.

This article examines five of the most common payment systems—checks, debit cards, ACH debits, wire transfers, and credit cards—and their general rules for allocating losses prior to and after execution of a payment transaction. The final section of this article considers recent developments in society and technology, notably the problems of Internet security and identity theft. This article asks whether the divergent approaches taken to the problem of unauthorized payment transactions should be unified. This article concludes by advocating, at least for small account holders, an approach based upon principles developed from the credit card system, even

9. Ronald J. Mann, *Making Sense of Payments Policy in the Information Age*, 93 GEO. L.J. 633, 638 (2005).

10. *Id.* at 638–39.

11. *Id.* at 638.

though these principles were not implicit in the minds of the drafters of the TILA.

The first step in the analysis is to briefly consider what the loss-allocation rules are for each of the five payment systems for pre- and post-transaction activities. This discussion is not meant to be exhaustive, but rather to highlight the differences in approach between the different payment systems.

I. CHECKING ACCOUNTS

A. Allocation of Losses Arising from Pre-transaction Activities

The basic rule is that an "item" such as a check must be "authorized" by the account holder; if it is not "authorized," the check is not "properly payable." In turn, if the check is not "properly payable," it cannot be "charge[d] against the account of a customer."[12] As the official comments to the U.C.C. note, a check "containing a forged drawer's signature or forged indorsement is not properly payable."[13]

This basic rule is modified in two contexts where an account holder's own actions can play a role. The first context is where the account holder's "failure to exercise ordinary care substantially contributes to an alteration of an instrument or to the making of a forged signature on an instrument." In that event, the account holder cannot use the forgery or the alteration as a defense "against a person who, in good faith, pays the instrument or takes it for value or collection."[14] Section 3-406(a) of the U.C.C. does not apply, however, to forged indorsements. In addition, the party, normally the account holder's bank, asserting the negligence of the account holder has the evidentiary burden of proving this negligence.[15]

The second context is the special rule for responsible employees, which is a strict liability rule rather than a negligence rule. Under section 3-405 of the U.C.C., the "fraudulent indorsement" of either the employer or the payee is "effective" if it is made by "an employee with responsibility with respect to the instrument," thus putting the loss on the employer.[16]

12. U.C.C. § 4-401(a) (2005).

13. *Id.* § 4-401 cmt. 1. Professor Rogers has written a thoughtful discussion of the forged facsimile signature cases. *See* Rogers, *supra* note 1, at 484–509. He discusses the standard agreement between customers and banks that places the burden on customers for any unauthorized signature if the signature is a facsimile and whether such agreements should be allowed to vary the provisions of Article 4.

14. U.C.C. § 3-406(a).

15. *Id.* § 3-406(c).

16. *Id.* § 3-405(b).

The policy behind this rule is 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."[17] It is, of course, possible for section 3-406 to apply if a signature is involved or the indorsement is carried out by an employee without "responsibility" with respect to instruments.

In both contexts, the negligence of the account holder's bank can absolve, on contributory negligence principles, the account holder of some of the loss.[18] As a practical matter, such negligence would be very difficult (if not impossible) for an account holder to prove.[19]

B. Allocation of Losses Arising from Post-transaction Activities

Checking accounts are subject to section 4-406 of the U.C.C. and its requirement that "the customer must exercise *reasonable* promptness in examining the statement or the items" for any "alteration" or unauthorized signature.[20] Failure to examine the checking account subjects the customer to liability under subsections (d)(1) and (d)(2). In addition, failure by the customer to report an unauthorized check "within one year after the statement or items are made available to the customer" precludes the customer from reversing the unauthorized transaction.[21]

"Reasonable" in subsection (b) assumes an economically rational actor who understands that she should be examining her statements. It does not assume the actual human beings who use checking accounts, and who often do not notice discrepancies. The stories of customer neglect are, anecdotally, overwhelming in number. One posting on a blog about Internet security reported that the author, in going through his deceased mother's banking account, found a recurring charge for $75 that had been withdrawn from the account each month by a pornography website. This withdrawal

17. *Id.* § 3-405 cmt 1.

18. *Id.* §§ 3-405(b), 4-406(e).

19. The customer not only has the burden of proof, but must also show that the bank "fails to exercise ordinary care," *id.* § 3-405(b), or "failed to exercise ordinary care," *id.* § 4-406(e). "Ordinary care" is defined in section 3-103(a)(9), which applies to Article 4 via section 4-104(c), as the "observance of reasonable commercial standards, prevailing in the area in which the person [e.g., the bank] is located, with respect to the business in which the person is engaged [e.g., banking]." *Id.* § 3-103(a)(9). In other words, the banks themselves get to define what "ordinary care" is. There is little room for a customer to argue that a bank should do anything. The only fruitful argument is that a bank failed to do something that most other banks in the area do.

20. *Id.* § 4-406(c) (emphasis added).

21. *Id.* § 4-406(f).

had been going on for five years without either of the author's parents being aware of it.[22]

Another way of understanding section 4-406's requirement that a customer act with "reasonable promptness" is to look at this requirement as a means of allocating blame. In fact the whole concept of "reasonable" has echoes of torts and of comparative negligence, which is also found in the pre-transaction context as discussed above.

The same type of provision requiring the customer to pay attention to her statements occurs in many of the more modern payment systems. The great exception is the credit card system, which is briefly discussed below, although there is some recent case law (particularly in the Second Circuit) that qualifies this generalization. But most other modern payment systems seem to have adopted a modified version of section 406 of the U.C.C. and its concept that a customer's failure to respond to a statement showing the unauthorized transaction should leave the loss with the customer.

II. DEBIT CARDS AND THE ELECTRONIC FUND TRANSFER ACT

The rights within section 909 of the EFTA apply, of course, only to transfers of funds involving accounts "established primarily for personal, family, or household purposes."[23] In other words, any business account would be excluded.

A. Allocation of Losses Arising from Pre-transaction Activities

Section 909 of the EFTA first provides a strict upper limit of $50 on the loss that can be allocated to an account holder for any "unauthorized electronic fund transfer."[24] The amount of the loss for which an account holder can be held liable increases to $500 if (a) the account holder fails "to report any loss or theft of a card . . . within two business days after the consumer learns of the loss or theft (or in extenuating circumstances such as extended travel or hospitalization, within a longer period which is reasonable in the circumstances)" and (b) "the financial institution establishes [that the loss] would not have occurred but for the failure of the consumer to report the loss or theft."[25]

22. Posting of Anonymous (June 9, 2006, 17:22 PST) to Schneier on Security, http://www.schneier.com/blog/ (Apr. 15, 2005, 09:17 PST) [hereinafter Schneier on Security].

23. Electronic Fund Transfer Act § 903(2), 15 U.S.C. § 1693a(2) (2000).

24. *Id.* § 909(a).

25. *Id.* § 909(a)(2).

B. Allocation of Losses Arising from Post-transaction Activities

A debit card holder, whose account is subject to the Electronic Fund Transfer Act, has to notify her bank "within sixty days of the transmittal of the statement (or in extenuating circumstances such as extended travel or hospitalization, within a reasonable time under the circumstances) [of] any unauthorized fund transfer" or lose her right to "reimbursement" for losses that would have been prevented by such notice.[26]

The EFTA's statement rule is less harsh than section 4-406 of the U.C.C. No reimbursement need be made to the account holder if the conditions of section 4-406 are met. In contrast, any losses over $50 that would not have been prevented by notice from the account holder (either within two days of knowledge of the loss or theft of the debit card or within sixty days of the transmittal of a statement) must be reimbursed by the bank under section 909(a) of the EFTA.

III. ACH DEBITS

A. Allocation of Losses Arising from Pre-transaction Activities

Although the ACH Rules do include the concept of an unauthorized credit or debit entry, there is no provision (except for one covering unauthorized debits from consumer accounts) that gives a general right to an account holder to not pay an unauthorized transaction.

Section 8.6 governs an account holder's right to have an unauthorized debit reversed. As with debit cards and the EFTA, the rights under subsection 8.6.1, which would apply to most debits, only arise with respect to a "Consumer Account,"[27] which is defined as "an account . . . established by a natural person primarily for personal, family or household and not for commercial purposes."[28] Once again, any business account would be excluded.

B. Allocation of Losses Arising from Post-transaction Activities

Unauthorized ACH debit transactions must be reported by the Receiver (i.e., the account holder) to the Receiving Depository Financial Insti-

26. *Id.*

27. NAT'L AUTOMATED CLEARING HOUSE ASS'N, 2007 ACH RULES: A COMPLETE GUIDE TO RULES AND REGULATIONS GOVERNING THE ACH NETWORK, § 8.6.1, at OR 28 (2007) [hereinafter 2007 NACHA RULES].

28. *Id.* § 14.1.20, at OR 41.

tution (RDFI) "within 15 calendar days from the date the RDFI sends or makes available to the Receiver information relating to the debit entry."[29] If such a report is not made, the RDFI is not obligated to "promptly credit the amount" of the debit entry. In other words, the RDFI is given a safe harbor from Receiver claims that the transaction was unauthorized. In addition, the report must be a "written" affidavit in a prescribed format.[30]

Similar provisions would apply to a POP transaction involving a consumer account.[31] A POP transaction is a one time point-of-sale transaction involving the conversion of a "source document" (e.g., a check)[32] into an electronic form. The "source document" must be "provided to the Originator by the Receiver at the point-of-purchase to effect a transfer of funds from an account of the Receiver."[33]

The closest provision that would apply to businesses is found in section 2.5, and even this section would only be useful in the event of an unauthorized credit from an Originator's account. Section 2.5 provides that an "erroneous entry" may be corrected if the "reversing entry" is "transmitted to the Receiving ACH Operator in such time as to be transmitted or made available to the RDFI by midnight of the fifth banking day following the Settlement Date of the erroneous entry."[34] An "erroneous entry" includes both an entry that "orders payment to or from a Receiver not intended to be credited or debited by the Originator" and an entry that "orders payment" in the wrong amount.[35] An exercise by the Originator (e.g., an account holder) of its right under subsection 2.5.2 triggers an obligation of the Originating Depository Financial Institution (e.g., the account holder's bank) to provide an indemnity to all financial institutions and the ACH Operator in the chain of payment orders from the Originator to the Receiver.[36]

29. *Id.* § 8.6.1, at OR 28.
30. *Id.* §§ 8.6.1., 8.6.5, at OR 28–29.
31. *Id.* § 8.6.2, at OR 28.
32. *Id.* § 3.7.2, at OR 17.
33. *Id.* § 14.1.48, at OR 43.
34. *Id.* § 2.5.1, at OR 8.
35. *Id.*
36. *Id.* § 2.5.2, at OR 8. Contractual arrangements between the ODFI and the Originator could provide for the Originator to indemnify the ODFI, in turn, for the indemnity required by the ACH rules.

IV. WIRE TRANSFERS AND ARTICLE 4A

A. Allocation of Losses Arising from Pre-transaction Activities

Insofar as Article 4A applies to a wire transfer, it provides an incentive to the bank that receives a payment order from an Originator (i.e., the account holder) to create a security procedure to ensure that the payment order is authorized. If the receiving bank puts in place "a commercially reasonable method of providing security against unauthorized payment orders" and "compl[ies] with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer," even an unauthorized payment order will be treated as if it were authorized.[37] If the receiving bank does not put in place a commercially reasonable security procedure, it would have the evidentiary burden of proving that an allegedly unauthorized payment order was in fact authorized,[38] a burden that could be very difficult to meet.[39] As the official comments to section 4A-203 state, "If a commercially reasonable security procedure is not made available to the customer, subsection [4A-202](b) does not apply. . . . [T]he bank acts at its peril in accepting a payment order that may be unauthorized."[40]

It is also possible for an Originator to choose a security system not designed by the receiving bank and for that security system to be "commercially reasonable." For such a procedure to be reasonable, it must be chosen only "*after* the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer."[41] In addition, the Originator must "agree[] in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer."[42] The practical effect of such a provision would seem to be to encourage a customer to accept a security system designed by the receiving bank in order to avoid the costs of developing its own system.

The drafters of Article 4A expected receiving banks to develop the security systems and designed Article 4A to impose on the receiving banks "[t]he burden of making available commercially reasonable security proce-

37. U.C.C. § 4A-202(b) (2005).

38. *Id.* § 4A-202(a).

39. Jane Kaufman Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1229–30 (1998).

40. U.C.C. § 4A-203 cmt 3.

41. *Id.* § 4A-202(c) (emphasis added).

42. *Id.*

dures . . . because they . . . are in the best position to evaluate the efficacy of procedures offered to customers to combat fraud."[43] This choice certainly makes sense if we think of the receiving banks as the experts in the field of wire transfers and, therefore, the best parties to develop proper security procedures.

In contrast, "[t]he burden on the customer is to supervise its employees to ensure compliance with the security procedure and to safeguard confidential security information and access to transmitting facilities so that the security procedure cannot be breached."[44] This is, of course, the imposition on the account holder of what is, in effect, a strict liability principle. The account holder can no longer argue, as she could with a checking account, that she took all the appropriate measures to prevent an unauthorized transaction. In addition, it is no longer the bank's burden to prove that the account holder was negligent.

The one argument that the account holder will have left is that the bank itself was negligent although, as with the checking system, this is a very difficult (if not impossible) thing for the account holder to prove.[45]

B. Allocation of Losses Arising from Post-transaction Activities

The bank statement rule for wire transfers is found in U.C.C. section 4A-505, which creates a "statute of repose" for receiving banks.[46] If an Originator receives "notification reasonably identifying the order," the Originator has one year "after notification was received" to notify the receiving bank of "the customer's objection to the payment." If the Originator fails to do so, then the Originator "is precluded from asserting that the bank is not entitled to retain the payment."[47]

43. *Id.* § 4A-203 cmt 3.

44. *Id.*

45. *Id.* § 4A-203(a)(2). The official comment notes that the "confidential information [necessary to institute an unauthorized payment order] must be obtained either from a source controlled by the customer or from a source controlled by the receiving bank." *Id.* § 4A-203 cmt. 5. The customer has the burden of "prov[ing] that the person committing the fraud did not obtain the confidential information from an agent or former agent of the customer or from a source controlled by the customer." *Id.* The official comment assumes that there would be criminal and bank internal investigations of any unauthorized payment order because of the large sums of money involved and that the customer would have access to the results. *Id.* Although the comment does not explicitly say so, presumably the prediction that such investigations would occur is meant to assuage doubts as to how a customer could ever meet her burden of proof.

46. *Id.* § 4A-505 cmt.

47. *Id.* § 4A-505.

V. CREDIT CARDS

A. Credit Cards and the Truth-in-Lending Act

Credit cards provide almost complete protection to consumers and many small businesses against unauthorized transactions. Section 133(a)(1) of the TILA imposes a series of conditions that a card issuer must meet before it can impose liability upon a cardholder. But in no event can a cardholder be liable for more than $50 "for the unauthorized use of a credit card."[48]

Although most provisions of the TILA do not apply to "extensions of credit primarily for business, commercial, or agricultural purposes . . . or to organizations,"[49] section 133 does apply to a card issuer and a business or organization that has nine or fewer employee card holders with that card issuer's card. In theory, section 133 could apply to any business or organization, but it provides that a card issuer and a business or organization can agree to exclude the operation of section 133 if the business or organization has ten or more employees with that issuer's card.[50]

The irony of the protection against unauthorized transactions above $50 that is built into the credit card system for consumers and many small businesses is that the protections grow out of a conception in the early 1970s that credit card use above a certain dollar limit is really an extension of credit, rather than a use of the card as a payment system.[51]

B. The Erosion of the Truth-in-Lending Act

In 1996, the Court of Appeals for the Second Circuit looked to section 4-406 of the U.C.C. for negligence principles that should, in that court's view, be applied to credit cards.[52] Although the facts in *Minskoff v. American Express Travel Services* are particularly extreme, and the Second Circuit used a circuitous route to arrive at its holding, the result is that a statement rule, with the associated concept of negligence, is creeping into the law of unauthorized credit card payment transactions.[53]

48. Truth in Lending Act, § 133(a)(1)(B), 15 U.S.C. § 1643(a)(1)(B) (2000).

49. *Id.* § 104(1).

50. *Id.* § 135.

51. *See* Roland E. Brandel & Carl A. Leonard, *Bank Charge Cards: New Cash or New Credit*, 69 MICH. L. REV. 1033, 1059–64 (1971).

52. Minskoff v. Am. Express Travel Serv., 98 F. 3d 703 (2d Cir. 1996).

53. *See* DBI Architects, P.C. v. Am. Express Travel-Related Serv. Co., 388 F.3d 886 (D.C. Cir. 2004); Carrier v. Citibank (S.D.), N.A., 383 F. Supp. 334 (D. Conn. 2005), *aff'd*, 180 Fed. App'x 296 (2d Cir. 2006).

Minskoff revolved around the question of whether a series of fraudulent credit card transactions were "authorized" because section 133 of the TILA provides that "[a] cardholder shall be liable for the *unauthorized* use of a credit card only if . . . the liability is not in excess of $50."[54] The account involved in *Minskoff* was a corporate account that was used by one of the corporate employees to carry out over $300,000 in fraudulent transactions over a three year period.[55] During this period, the president and chief executive of the company did not look at the twenty-eight credit card statements that showed both the name of the corporate employee and her charges, nor did he look at any of the cancelled checks that were used to pay for the charges.[56]

The *Minskoff* court looked at the definition of "unauthorized use" in the TILA[57] and noted that it provides that the term "means a use of a credit card by a person other than the cardholder who does not have actual, implied, or *apparent* authority for such use and from which the cardholder receives no benefit."[58] Looking to common law notions of apparent authority, the *Minskoff* court held that the card issuer was entitled to rely upon the apparent authority of the employee; therefore, section 133 did not dictate that the card holder had no liability beyond the $50 limit. "A cardholder's failure to examine credit card statements that would reveal fraudulent use of the card constitutes a negligent omission that creates apparent authority for charges that would otherwise be considered unauthorized under the TILA."[59]

The *Minskoff* court relied upon the policy embodied in section 4-406 of the U.C.C., the bank statement rule, that whoever is in the best position to detect a forgery or alteration should be liable for it. The court, by characterizing this statutory provision as "derived from a common law obligation"[60] was, by extension, also characterizing the policy as one favored by the common law.

The opinion did distinguish between the obtaining by the employee of new cards and the transactions on these cards. "[T]he *acquisition* of a credit card through fraud or theft cannot be said to occur under the apparent authority of the cardholder . . . ."[61] Sometime between the employee's "initial

54. Truth in Lending Act § 133(a)(1), (a)(1)(B) (emphasis added).
55. *Minskoff*, 98 F.3d at 706–07.
56. *Id.*
57. *Id.* at 708.
58. *Id.* (citing Truth in Lending Act § 103(o)) (emphasis added).
59. *Id.* at 709–10.
60. *Id.* at 709.
61. *Id.*

possession" of the unauthorized credit cards and their "subsequent *use*," negligent acts by the card holder can create apparent authority.

To date, the *Minskoff* approach has only been applied to credit card accounts held by businesses. But there is nothing in the reasoning of this case and the handful of other cases that have considered card holder negligence that would prevent the apparent authority principle from being applied to fraudulent use of a consumer credit card by a family member, friend, or acquaintance of the card holder.

VI. HOW PRIVACY AND IDENTITY THEFT IMPACT THE CURRENT LOSS-ALLOCATION RULES

It is important to place the legal rules that have evolved into their historical context. The rules for checking accounts, embodied in Articles 3 and 4 of the Uniform Commercial Code, evolved in world in which a limited number of people had checking accounts and in which the transaction had to be initiated with a piece of paper that had been physically signed. In addition, if you were an individual, it was unlikely that you had more than two accounts—a checking and, in some cases, a savings account.[62]

Today, we live in a world where the numbers of account holders, the accounts per holder, and the numbers (and types) of transactions involving cards and electronic transfers have expanded exponentially.[63] For example, a much larger percentage of United States households now have at least one credit card as compared to the situation in 1969.[64] In addition, the debit card is a relatively recent innovation.[65]

62. *See* Robert D. Bowers, *Businesses, Households, and Their Banks*, *in* BANKING MARKETS AND FINANCIAL INSTITUTIONS (Thomas G. Gies & Vincent P. Apilado, eds., 1971). Most small businesses "in central Bucks County [Pennsylvania] used a single commercial bank for all of their banking needs" and "the typical bank-business relationship is one of long standing." *Id.* at 271–72. Nationally in 1967, only 68% of households in the United States even had a checking account. *Id.* at 273.

63. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-06-929, CREDIT CARDS: INCREASED COMPLEXITY IN RATES AND FEES HEIGHTENS NEED FOR MORE EFFECTIVE DISCLOSURES TO CONSUMERS 9, 10 (2006) (discussing credit cards). The best source of credit card data, CardWeb.com, does not allow legal academics to access its data. The GAO, however, was able to access that data and reports that the number of credit cards in use has grown from considerably less than 100 million in 1980 to more than 691 million by 2005. *Id.* at 9, 10 fig.1. The yearly charge volume has increased approximately six times from 1980 to 2005, from approximately 300 billion dollars to more than 1.8 trillion dollars. *Id.* at 1, 9. In 1970, there were approximately 300 million outstanding credit cards, including 150 million independent retailer cards, 50 million bank credit cards, 6 million travel and entertainment cards, 1.5 million air travel cards, and 13 million miscellaneous credit cards. H.R. REP. No. 91-1500, at 7 (1970).

64. In 1969, approximately 25% of households had a bank credit card. This percentage increased to 48.3% for households with post-graduate college education. Robert Johnston, *Credit and Credit Cards*, *in* BANKING MARKETS AND FINANCIAL INSTITUTIONS, *supra* note 62, at 258. In 2001, 76.2% of all households had credit cards (72.7% had bank cards); 47% used debit cards; and 69.8% had ATM cards (which, of course, might overlap with the debit card category). Elizabeth Klee, *Families' Use of*

The changing means of making payments has greatly complicated the issue of security for an account holder. In a paper-based check world, protecting a single checkbook or savings passbook would provide a reasonable certainty to the account holder that an unauthorized transaction could not occur. Similarly, when credit cards first became widely available in the United States in the 1960s, most transactions were conducted in person, with the card physically present.[66] As she could in a paper-check world, a small account holder could achieve reasonable security by ensuring that her credit card never left her physical possession.[67] Indeed, the Federal Reserve Board official staff commentary on Regulation Z, which implements the TILA, interprets the requirement that a "card issuer has provided a means to identify the cardholder on the account or the authorized user of the card"[68] as implying that the card be physically present when a charge is made.[69] Today an unauthorized transaction involving a bank account, credit card, or any other account holding financial assets or providing access to financial assets requires only access to a limited amount of information concerning the account and its holder. Not surprisingly, the number of such incidents and the aggregate amounts involved in such incidents has grown markedly over the past ten years.

A couple of illustrations from current litigations show the ease with which access can be obtained to another person's financial accounts. The first is the case of the *United States of America v. Payment Processing Center, LLC*. The alleged scheme was described as:

Payment Instruments During a Decade of Change in the U.S. Payment System 21 tbl.2(a) (Bd. Of Governors of the Fed. Reserve Sys., Fin. & Econ. Discussion Series, Paper No. 2006-01, 2006), *available at* http://www.federalreserve.gov/pubs/feds/2006/200601/200601pap.pdf.

65. David A. Balto, *Can the Promise of Debit Cards be Fulfilled?*, 53 BUS. LAW 1093, 1093 (1998) ("Another payment system—debit cards—was relatively uncommon in the United States until the mid-1990s.").

66. Rogers, *supra* note 1, at 497 ("At one time, no merchant would accept a credit card payment without obtaining the signature of the user.").

67. Where credit card transaction are conducted in person, "use of the card depends on physical possession of the card" and "the customer can reduce the risk by taking good care of the card and promptly reporting its loss. Taking care of articles like cards or keys is largely a matter of common sense (to be contrasted with the precautions required to protect electronic systems . . . .)" Nicholas Bohm, Ian Brown & Brian Gladman, *Electronic Commerce: Who Carries the Risk of Fraud?*, J. OF INFO. L. & TECH., Oct. 31, 2000, at 4, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm.

68. Truth in Lending (Regulation Z), 12 C.F.R § 226.12(b)(2)(iii) (2007).

69. 12 C.F.R. pt. 226, supp. I, § 226.12, para. (b)(2)(iii), notes 1 & 3. The commentary gives as examples of adequate "means to identify" the following: "signature, photograph, or fingerprint on the card, or electronic or mechanical confirmation." *Id.* at note 1. The "card itself (or some other sufficient means of identification of the cardholder)" must be "presented" in order for the cardholder to be liable for a transaction. In a sense, the commentary is treating the "means to identify" as an evidentiary basis for finding that an unauthorized transaction has occurred. A cardholder would not, for example, be liable for an unauthorized transaction "when merchandise is ordered by telephone by a person . . . using a credit card account number or other number only (which may be widely available)." *Id.* at note 3.

> [A] complex and sprawling scheme involving the seven individual defendants and a corporate defendant, hundreds of thousands of victims who are dispersed throughout the country, hundreds of thousands of fraudulent transactions, dozens of domestic and foreign telemarketers operating under innumerable fictitious names, and tens of millions of dollars of consumers' money being transferred to banks in the United States and abroad.[70]

The scheme made use of remotely created checks drawn on the accounts of senior citizens.[71] Senior citizens are particularly fruitful targets, because illness often prevents them from realizing that a fraud is occurring. In addition, even when a senior citizen realizes that a fraud is occurring, she may be afraid to seek help, because her relatives may take control of her financial life away from her.[72]

The second is a securities fraud action brought by the Securities and Exchange Commission, *SEC v. Kamardin*.[73] Although *Kamardin* did not involve payment systems, it does highlight the vulnerability to hacking of computer systems maintained by financial institutions. In this case, one individual was allegedly able to "surreptiously usurp[] the online trading accounts of the victim investors at various broker-dealers, liquidate[] the investors' existing equity positions, and us[e] the resulting proceeds [to] purchase[] thinly-traded stocks in the investors' accounts in order to create the appearance of trading activity and to inflate the price of the stocks."[74]

70. United States of America's Memorandum in Opposition to the Defendants' Motion to Dissolve the Asset Freeze at 4, United States v. Payment Processing Center, LLC, No. 06-00725 (E.D. Pa. Dec. 8, 2006).

71. Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. TIMES, May 20, 2007, at 1. *See generally* Kurt Summers, Note, *Remotely-Created Checks; Legislative Reluctance, Reciprocity Requirements, and the Federal Rule that Changes Everything*, 38 TEX. TECH. L. REV. 1179 (2006) (describing remotely-created checks and the 2005 amendment to Regulation CC defining "remotely created checks" and creating transfer and presentment warrants for such checks).

72. Duhigg, *supra* note 71. Duhigg describes the plight of Richard Guthrie, who allegedly lost more than $100,000. The first step was for a telemarketing firm to create a list of senior citizens. Mr. Guthrie enjoyed the calls from telemarketing employees. "I really enjoy when those salespeople call. But when I tell them I can't buy anything now, they hang up. I miss the good chats we used to have." The telemarketing firm then sold the list to a criminal, who used various pretexts during telephone calls to senior citizens on the list to gain banking data for the senior citizens. *Id.*

73. U.S. Sec. & Exch. Comm'n v. Kamardin, No. 8:07-cv-159-T-24-MAP, 2007 U.S. Dist. LEXIS 44260 (M.D. Fla. June 19, 2007). The scheme was a pump-and-dump scheme whereby Kamardin used the compromised accounts to purchase shares in "thinly-traded issuer[s]," thereby driving up the price of the shares. Once the price had been driven up, Kamardin sold shares he had already purchased at inflated prices. Complaint for Injunctive and Other Relief at 1, *Kamardin*, 2007 U.S. Dist. LEXIS 44260 (No. 8:07-cv-159-T-24-MAP). The defendant transferred his profits, and evidently fled, to Russia.

74. Complaint for Injunctive and Other Relief, *supra* note 73, at 1.

The broker-dealers at which the compromised accounts were located included major broker-dealers.[75] The scheme went on for six weeks.[76]

To make matters even more complicated, the limited amount of information necessary to initiate an unauthorized transaction is held not only by the account holder and the financial institution at which the account is located, but by numerous third parties such as credit card merchants with which the account holder has interacted. The account holder can do nothing to protect this information from being stolen electronically from such institutions' computers or from being stolen physically. To take just one example, a recent article in *The Wall Street Journal* reported that restaurants are one of the most fertile grounds for the theft of credit card details.[77] Although the credit card industry has security protocols that all merchants are supposed to follow, "'There are tens of thousands of restaurants that aren't complying' with industry security rules."[78] The result is that, "[s]ince January 2005, restaurants represented about 40% of incidents in which intruders gained unauthorized access to credit-card information, according to data tracked by Visa." A firm that "conducts security audits for merchants . . . says that 62% of the security breaches it has seen over the past 18 months came from the restaurant industry."[79]

The examples of losses of personal data by (and thefts of personal data from) third parties are myriad. News articles appear weekly reporting that the private information of thousands, often more, of account holders has been jeopardized. One website publishes a chronological list, which is usually updated twice a week, of data breaches reported in the U.S. from 2005 through 2007. As of April 5, 2007, the list was sixty-one pages in length and included data breaches involving 150,520,490 records that contained "data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers."[80] The overall number of

75. "The accounts were intruded into at various broker-dealers, including E*Trade Securities, Scottrade, Inc., TD Ameritrade, Inc., J.P. Morgan Chase & Co. and Charles Schwab & Co., Inc." *Id.* at 4.

76. *Id.* at 2. The automation of a pump-and-dump scheme by use of computers has some parallels with how a payment systems fraud could be expedited, but is even more striking because a pump-and-dump scheme usually requires multiple bad actors who act over an extended period of time. "What historically required legions of con artists and days or even weeks of planning and execution was in this instance accomplished single-handedly or by a small group within only minutes." *SEC Pursues Alleged Perpetrator of Market Fraud Using Others' Accounts,* 39 Sec. Reg. & L. Rep. (BNA) 135–36 (Jan. 29, 2007) (quoting John Reed Stark, Chief of the SEC's Office of Internet Enforcement).

77. Robin Sidel, *Card Companies Crack Down on Restaurants: Diners' Personal Data Not Well Protected, Visa and Others Say*, WALL ST. J., Mar. 24–25, 2007, at B1.

78. *Id.* (quoting Robert Carr, CEO of Heartland Payment Systems Inc.).

79. *Id.*

80. Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Mar. 6, 2008).

records does not necessarily reflect the number of individuals affected as "[s]ome individuals may be the victims of more than one breach." But the compilers of the list believe that "[i]n reality the number given below [for records involved in data breaches] should be much larger. For many of the breaches listed, the number of records is unknown."

Some of this stolen or lost information would allow the thief to institute unauthorized transactions directly; some of this stolen or lost information would allow the thief to attempt such a transaction only if she found additional information about the account holder. This information could be obtained through deceptive telephone calls or e-mails or even through publicly available information on the Internet.

Most identity theft involves someone that the victim knows. But criminals are becoming more and more involved. In addition, unauthorized transactions have moved from the realm of the individual criminal to the realm of organized crime. There is one gang operating out of Russia, the Rocky Gang, that has a minimum of twelve members and that took in more than an estimated $150 million in 2006.[81]

The structure of the Internet itself helps create the myriad security problems. The Internet is structured so that the end points of the networks, the computers (PCs in the case of individuals and most small businesses), are usually designed to be open to computer programs from any source rather than from a limited range of controlled sources.[82] Combine this openness with a resistance to any control over the content on the Internet, i.e., end-to-end neutrality,[83] and with continual access by high speed connection of PCs to the Internet,[84] and you create a situation in which the PC owners lose control of their own computers unless the PC owners possess unusual technical competences.[85]

The most that an account holder can do is to try to make her own Internet access devices, including her computers, relatively secure and, if she has received physical records of her accounts, to make sure that these records are either physically secure and in her possession or physically destroyed in a manner that makes the information contained within them unreadable. The first piece of bad news is that she does not in any real

81. Arjen de Landgraaf, *The Almost Perfect Bank Heist*, FIN. TIMES (U.S.A), Mar. 14, 2007, Digital Business Special Report, at 3.

82. Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1983–84 (2006).

83. *Id.* at 1988.

84. *Id.* at 1995.

85. *Id.* at 2003–05. To properly secure PCs, the owners would have to know "how to manage or code their PCs . . . [and] to apply patches rigorously [and to] observe good password security." *Id.* at 2005. Few PC owners have such skills.

sense control her operating system, browser, or other crucial software and that there is a high level of expertise necessary to deal with security problems.

As to the operating system, the most widespread ones are versions of Microsoft Windows. And, as anyone who has used Windows knows all too well, there have been numerous security problems involving versions of Windows. A similar set of security problems has been created by Microsoft's Internet browser, Explorer, which is the most widely-used browser. As of April 9, 2007, one website that specializes in security issues in software has approximately 1710 postings, each describing a different security vulnerability in a Microsoft product.[86] It is unrealistic to expect any individual to spend the energy necessary to keep up with these security problems, much less try to run all the patches necessary to fix them.

Security experts suggest that the typical individual computer user at a minimum should do the following to make her personal computer more secure: "Install and regularly update firewall, anti-spyware, anti-virus and browser security software if you have a home computer." If you are using public computers, "ensure that they are equipped with appropriate security software."[87] How many of the readers of this article carry out all these steps? And how many of you even know what "appropriate security software" would be on a public computer, much less be able to find it if you did know? On an anecdotal level, I certainly do not carry out all of these steps and I have no idea what security software a public computer should contain.

It is not surprising that some writers about online security issues recognize that it is unrealistic to expect most individual computer users to take adequate technical measures to protect against identity theft. The victims of online fraud "should install firewalls and have adequate virus protection—but they often do not. And an inability to use technology safely and poor appreciation of the risks involved, [sic] makes consumers doubly vulnerable."[88]

In the United Kingdom, a committee of the House of Lords, in a recent report,[89] stated that "[t]he current emphasis of Government and pol-

86. SecurityFocus, Home Page, http://www.securityfocus.com/bid (last visited Mar. 6, 2008).

87. JAVELIN STRATEGY & RESEARCH, 2007 IDENTITY FRAUD SURVEY REPORT—CONSUMER VERSION: HOW CONSUMERS CAN PROTECT THEMSELVES 5 (2007), *available at* http://www.javelinstrategy.com/research/all (scroll down to "February 2007").

88. Peter Cochrane, *Banking Fraud—We Need the Will to Stop It*, FIN. TIMES (U.S.A), Mar. 14, 2007, Digital Business Special Report, at 2.

89. SCIENCE AND TECHNOLOGY COMMITTEE, HOUSE OF LORDS, PERSONAL INTERNET SECURITY, 2006-7, H.L. 165-I, *available at* http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf.

icy-makers upon end-user responsibility for security bears little relation either to the capabilities of many individuals or to the changing nature of the technology and the risk."[90] Based on these realities, the committee recommended that internet service providers should be liable "once ISPs have detected or been notified of the fact that machines on their network are sending out spam or infected code"[91] and that consideration be given to making software and hardware manufacturers liable for damage arising out of security problems.[92] Although the remedies proposed by the committee are beyond the scope of an article about payment systems, they should remind us of how serious these issues are and prompt consideration of who is the proper party to control technological risk.

If the account holder uses only a computer with a fixed telephone line at predictable hours, this gives the financial institution three pieces of information to use to verify the account holder. Even if the account holder were to use a work computer, this is only one additional access device, although the account holder would not control this computer. Combine these three pieces of information with a user name and password (or PIN) and you have a five-factor security system that is difficult to penetrate. But we have moved to a world of two-factor identification (user name and password), driven by the technological changes that allow account holders to access their accounts in many different ways, the social changes that favor constant and universal connection to the Internet, and the competition between financial institutions to accommodate their account holders.

The issues with how access to accounts is changing will just become more and more serious, especially as new means of accessing accounts are created. As one journalist described the current situation:

> People increasingly access bank accounts on the hoof, gaining access over the internet by local area networks, Wi-Fi, or 2.5/3G mobile connections from multiple locations and multiple terminals. PCs, laptops, PDAs and other mobile devices equipped with browsers access bank accounts from anywhere, including the home, office, internet cafe, airport lounge, hotel bedroom and public kiosks.[93]

The journalist could have added that the accounts with financial assets that are accessed in this fashion are not limited to bank accounts.

The possible access devices just keep multiplying. Citibank, for example, has introduced a new product, Citi Mobile, that allows access to a bank account through a cell phone. The product is available "on a wide

90. *Id.* at 80.
91. *Id.* at 81.
92. *Id.* at 82.
93. Cochrane, *supra* note 88.

range of phones" and Citibank's website reports that "more [are] on the way." All information will be protected by 128-bit encryption.[94] The ability of a thief to intercept the information, however, will be greatly increased by her ability to intercept it in e-mail transmitted through a wired network.

The greatly expanded means of an account holder's communicating with her financial institutions creates not only increased opportunities for technical interception of account information, but also increased opportunities for thieves to physically observe account holders using passwords and user names.

Losses of personal information can trigger three types of identity theft: "unauthorized use or attempted use of existing credit cards," "unauthorized use or attempted use of other existing accounts such as checking accounts," and "misuse of personal information to obtain new accounts of loans, or to commit other crimes."[95] The first two categories, of course, implicate one of the key concerns of payment systems: the allocation of losses for unauthorized transactions. In contrast, the third category is not one that the law of payment systems has historically addressed. The law of payment systems deals with unauthorized transactions involving existing accounts and the allocation of the losses arising from these transactions. But it has no special competence on what the legal consequences of a new account, opened with stolen information, should be.

The 2004 National Crime Victimization Survey, a national survey of a representative sampling of households conducted by the Bureau of Justice Statistics of the U.S. Department of Justice, reported that 1,736,700 households had experienced unauthorized use of existing credit cards and 896,500 households had experienced unauthorized use of other existing accounts.[96] These households constituted 2.3% of all U.S. households. Households with a household income of $75,000 or more and households headed by a person age 18–24 were most likely to suffer one of the three types of identity theft.[97] The reported losses suffered from the three types of identity theft were approximately $3.2 billion. "The losses reported include money that may have been reimbursed by others such as credit card companies or insurance companies and exclude such things as costs associ-

94. Citibank, Citi Mobile, http://www.citibank.com/us/index.htm (select "Introducing Citi Mobile" under "New and Noteworthy") (last visited Mar. 6, 2008).

95. KATRINA BAUM, U.S. DEP'T OF JUSTICE, IDENTITY THEFT, 2004, at 1 (2006), *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

96. *Id.*

97. *Id.* at 2 & tbl.1.

ated with paying higher interest rates and wages lost from time spent clearing up problems associated with the theft."[98]

Of great interest to thinking about how to allocate losses caused by unauthorized transactions is how households discovered the identity theft. Identity theft involving credit cards was discovered by 43.0% of households when they were "[c]ontacted about late/unpaid bills" (30.7%), experienced "[b]anking problems" (11.8%), "[n]otified by police" (0.4%), or "[d]enied phone or utility service" (0.1%).[99] The comparable percentage for unauthorized use of other existing accounts was 25.7%. The latter households discovered the theft when they were "[c]ontacted about late/unpaid bills" (9.0%), experienced "[b]anking problems" (11.7%), "[n]otified by the police" (0.6%), or "[d]enied phone or utility service" (4.4%). The comparable overall percentage for multiple types of theft—which would have had to include at least one of the two types of unauthorized use—during the same incident is 43.3%. In all three categories, there is a large residual percentage that learned of the theft in some other way, ranging from 19.3% (existing credit cards) to 35.2% (other existing accounts), with the multiple types of theft falling in between at 27.5%.[100]

It is interesting to note that households appear to have been more careful about accounts other than credit cards, as 25.7% of the households became aware of the theft through means that appear most clearly to have not been initiated by the households (an "external means"), while the comparable percentage for credit cards is 43.0%. Perhaps households have been motivated by the rules for allocating unauthorized losses to be more attentive to accounts other than credit card accounts.

The percentage of households that came to know of the theft through an external means is still quite large for either category. Why this should be so is briefly explored below.

As to the two moments at which losses could be prevented, upon which this article is focused (i.e., before the unauthorized first transaction, and subsequent to the first unauthorized transaction), regarding the first transaction, many computer security experts do not hold out much hope that account holders, at least small account holders, can or will do much to prevent unauthorized transactions using information stolen from their computers. These experts think the problem of unauthorized transactions should be reconceptualized. Instead of focusing on how to prevent access to an

98. *Id.* at 5.
99. *Id.* at 3 tbl.2.
100. *Id.*

account, they think that the problem is preventing the unauthorized transaction:

> The user's PC is possibly the worst place of all to try to secure the banking system, as the bank has no say whatsoever about what software is installed, who uses it, what other things are done with the machine and so on. It's a lost cause. I will say now that there is no way you can prevent access credentials from being stolen.[101]

As one computer security expert put it, "the user's PC . . . is owned by the phishers[,] I'm afraid."[102] One well known computer security expert has gone as far as to suggest that the basic model for allocating responsibility for unauthorized transactions should be the credit card system.[103] From his perspective, the important thing about the credit card system is that the allocation of losses has caused the credit card companies to focus on the proper thing, which is "verifying the transaction," rather than "verifying the cardholder or putting requirements on what he does."[104]

In part, this focus on policing the transaction and not the account holder is a technical matter, especially with respect to small account holders. The operating systems that make such theft all too easy are not created or controlled in a real sense by small account holders. In addition, even those technical solutions that exist and that are relatively affordable may be beyond the technical expertise of the small account holder. Finally, studies have shown that even relatively straight forward current security systems will not be used by small account holders.

One recent study examined security measures that financial institutions have taken against man-in-the-middle attacks and phishing.[105] The study involved three study groups, one of which played the role of an online banking customer, the second of which played this role but was told that account security was the subject of the study, and the third of which used their own accounts. All of the accounts were located at the same bank and the study gave the participants three clues that there might be security problems. The clues escalated in seriousness: the first was the presence of "http" instead of "https" on the bank's password-entry page, the second was the removal of the site-authentication image, and the third was a blunt

101. Paul McGowan, Gone Phishing . . . (May 5, 2005) (unpublished article, *available at* http://members.optusnet.com.au/paul.mcgowan/phishing.html); *accord* Schneier on Security, *supra* note 22.

102. McGowan, *supra* note 101.

103. Schneier on Security, *supra* note 22.

104. *Id.*

105. Stuart E. Schechter et. al, The Emperor's New Security Indicators: An Evaluation of Website Authentication and the Effect of Role Playing on Usability Studies (Feb. 4, 2007) (unpublished working draft), *available at* http://www.usablesecurity.org/emperor/emperor.pdf.

browser warning page that the participant should be careful. The latter went so far as to warn that "[s]ecurity certificate problems may indicate an attempt to fool you or intercept any data you send to the server."[106] Neither of the first two warnings significantly deterred the study participants from signing into their accounts. The third warning deterred 47% of the role-playing group that had received no information about the purpose of the study, 29% of the role-playing group that had received such information, and 55% of the group accessing their own accounts.[107] As the authors noted, "[p]articipants who used their own accounts in our study behaved more securely than those who were assigned to play roles."[108] This finding supports the common notion that some burden should be placed upon account holders to monitor unauthorized transactions. On the other hand, the percentage of account holders willing to ignore even the most blatant security warning—36%—is quite startling.

In part, the problem of what small account holders can do before an unauthorized transaction is a matter of behavioral economics. The results of the studies on security systems should not be surprising. Individuals use, for example, an availability heuristic, which relies upon how easy it is to bring to mind occurrences, and have a "self serving" bias of overconfidence.[109] This article is not meant to be an in-depth exploration of the relevant behavioral economic issues. Rather, it merely means to suggest that biases of these kinds may contribute to the likelihood that small account holders will not take all of the protective measures that they should.

Finally, individual account holders have span of control problems. How can they keep track of their myriad of accounts? As a simple, anecdotal example, think about passwords that are used to access financial websites and the associated accounts online and other websites. I try not to have multiple passwords. I can barely remember a couple of variations much less the dozens that I would need to have unique passwords for each of my financial websites and the other websites on which I am registered. In fact, as I have had to generate different user names or passwords for one reason or another, I have had to create a written list that I keep near my PC. Anecdotally, mine is a common problem and a common solution that raises obvious security issues.[110] The problem is just becoming more convoluted

106. *Id.* at 5–6 & fig.1.

107. *Id.* at 9 tbl.5.

108. *Id.* at 10.

109. Jeffrey J. Rachlinski, *The Uncertain Psychological Case for Paternalism*, 97 NW. U. L. REV. 1165, 1170–73 (2003).

110. The Gripe Line, http://www.gripe2ed.com/ (May 4, 2007, 12:11 PDT).

as financial institutions add security questions (e.g., "your mother's maiden name") to websites.

In case anyone thinks that the multiplication of questions is increasing security, she should consider what computer security experts say. They point out "there are three ways to authenticate someone: by something he knows [e.g., passwords], by something he has [e.g., a physical card], and by something he is [e.g., biometrics like fingerprints]."[111] An authentication procedure that uses multiple items from the same category, e.g., a password and a mother's maiden name, is only marginally more secure than a procedure that uses one item. It is the use of items from more than one category that makes for strong authentication. And it is exactly this use of items from multiple categories that is missing in the online world.

The expectation that small account holders will systematically examine their myriad account statements for unauthorized transactions is similarly unrealistic. Small, recurrent transactions easily evade small account holder scrutiny. One reporter for *The New York Times*, who writes a regular column entitled "Online Shopper," reported on her expenses with a recurring charge of $10 that had been appearing on her credit card statement for sixteen months.[112] As she reports her own behavior, she avoids a careful scrutiny of her credit statements because "[t]ypically, my statements list so many troubling purchases."[113] By chance, she saw the $10 charge on a statement and then started researching it. Luckily, she was dealing with a reputable merchant, which refunded her all sixteen months' worth of charges.[114] What would have occurred, however, if she had been dealing with a fraudster? She could have lost her rights to a reversal of the charges under the *Minskoff* line of cases.[115]

The same span of control phenomenon occurs, of course, with outright fraud. One common fraud involving credit or debit cards is for a merchant (or someone working for a merchant) to take two scans of a card.[116] The second scan is used to produce a new card. This type of card fraud is called "card skimming."[117] So long as the withdrawals using the debit card are

111. Bruce Schneier, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 186 (2003).

112. Michelle Slatalla, *Who Charged This? You, That's Who*, N.Y. TIMES, Apr. 19, 2007, at G8.

113. *Id.*

114. *Id.*

115. *See supra* notes 52–61 and accompanying text.

116. Council of Better Business Bureaus, Inc., Who's Swiping Your Credit Card?, http://www.bbb.org/Alerts/article.asp?ID=316 (last visited Mar. 6, 2008).

117. *Id.*

small, they may well escape the scrutiny of a small account holder or, if the small account holder is a small business, of the responsible employee.[118]

CONCLUSION

This article is not meant to be an in-depth analysis either of the Internet's workings or of the problems of computer security. I do not have either the necessary expertise or space. Rather, this article is meant to suggest that the issue of who can police unauthorized payment transactions has become entangled with a series of technical issues about which many lawyers, myself included, have little knowledge. What we should be seeking is a set of principles for payments law that are not dependent on the current state of technology. One thing that we should all be able to agree upon is that the technology has exceeded the ability of most people to understand or control it, that this fact is unlikely to change, and that the complexity of technology will just keep increasing. This suggests that we should look to the financial institutions that participate in the payment systems to police them, including preventing unauthorized transactions.

A second thing that we should all be able to agree upon is that the sheer quantity of information concerning payments that an account holder must process has grown tremendously. This also suggests that account holders might be too easily overwhelmed to be effective monitors of unauthorized transactions.

It is time for a serious reconsideration of how losses for unauthorized transactions are allocated and whether there should be a unified approach, at least with respect to small account holders. The survival of negligence concepts in the checking system and in the various forms of the statement rule have left courts with room to allocate the losses from unauthorized payment transactions on an ad hoc basis.

The Article 4A model would place the burden upon financial institutions to create security systems, but would place the burden upon the account holders to police the use of these security systems. This allocation of responsibility may not make sense with respect to small account holders.

118. Interview with Michael Shorr, Chairman, Pendant Partners, Inc. (November 5, 2007). The withdrawals from the Pendant corporate account went on for five months, were occasional (no more than two times per month), and were never larger than $10. The employee who reconciled the bank statements did not want to trouble the Chairman by querying the Chairman about occasional withdrawals. She assumed that these were legitimate business expenses. The fraud did not come to light until a series of withdrawals of $29.99 and $34.99 were made, which were much larger than the prior withdrawals. In other words, the fraud did not come to light until the frequency and the amount of each withdrawal increased greatly. Luckily, the bank at which Pendant's account was located did not insist upon exercising its rights under section 903(4) of the EFTA and recredited Pendant's account for the fraudulent withdrawals.

Moving to the credit card model as the default model for payment systems would squarely place the burden upon financial institutions to deal with unauthorized transactions. This approach seems most in accord with the current technological and social realities.