ACH Payments: Changing Users and Changing Uses*

Policy Analysis Paper #6
October 2005

Karen Furst and Daniel E. Nolle
Policy Analysis Division
Office of the Comptroller of the Currency

Summary: Declining paper check usage, growing reliance on credit cards, and the rapid expansion of debit cards are all well-known aspects of the rise of electronic payments, but less focus has been placed on automated clearing house (ACH) transactions. This Policy Analysis Paper describes the changing ACH landscape, and considers the degree to which this growth and change have heightened one risk issue in particular: the susceptibility of ACH payments to fraud. The paper begins by summarizing overall trends in ACH payments and factors underlying the growing demand. This description of the ACH landscape also focuses on the emergence and rapid recent growth of a new set of ACH debit transactions, referred to as "e-checks" that, unlike traditional ACH debits, do not rely on established customer-originator relationships.

The addition of new ACH applications has attracted new participants, including third-party processors. Technological advancements have reduced scale and information processing barriers to entry for these third-party processors. As a result, the number and relative importance of third-party processors has increased along with the growth of the ACH network. The entry of new participants, in combination with attributes of some of the new ACH applications, increases the vulnerability of the system to fraud. Three long-standing characteristics of the ACH system have made it somewhat vulnerable to fraud, although historically ACH fraud rates have been low. These vulnerabilities include weak fraud detection and prevention mechanisms, weaknesses in the incentive structure for return items, and weak system governance. Added to these vulnerabilities is the increased complexity that results from the entrance of new third-party processors, which add one or more layers of participants between originating banks and the entities for whom those banks ultimately are originating ACH payments. It is possible this layering might diminish or eliminate the due diligence a bank would otherwise perform were it to have a direct customer relationship with the originator. In the absence of such due diligence, a bank may facilitate unauthorized withdrawals from consumer bank accounts by unscrupulous merchants engaged in deceptive or unfair acts and practices.

In response to an increase in fraud, industry and government authorities have introduced measures designed to prevent "bad actors" from entering the system, and to make it more difficult for those who do slip through the cracks to continue to exploit the ACH network. These measures, aimed specifically at counteracting existing vulnerabilities in the system's fraud detection and prevention mechanisms, emphasize better due diligence by participants with respect to originators that are being given access to the payments system.

*The views expressed in this paper are those of the authors, and do not necessarily reflect those of the Office of the Comptroller of the Currency or the Department of the Treasury.

Introduction

The financial services community and the business press have given increased attention to the significant shift in the balance between paper-based and electronic retail payments. Declining paper check usage, growing reliance on credit cards, and the rapid expansion of debit cards are all well-known aspects of the rise of electronic payments. Less focus has been placed on automated clearing house (ACH) transactions, but the growth in the use of this form of electronic payment and, more significantly, changes both in the nature of such payments and in the participants who make up the ACH system, warrant scrutiny.

Historically, ACH payments have been preauthorized arrangements between payors and payees, commonly in a sustained and systematically recurring manner (for example, automatic deposit of payroll and the pre-authorized monthly payment of an insurance premium). More recently, new applications have emerged – known collectively as "electronic checks" or "e-checks" – most of which, unlike traditional ACH payments, are not pre-authorized, and some of which are also characterized by the lack of an established relationship between the payor and the payee. Related to the transformation of the ACH network from one used primarily for recurring payments to a more general-purpose payments network is the role that third parties play in processing many of these new "e-check" payments. Frequently, these third-party processors stand between the bank and the merchant originating the payment, which can complicate customer due diligence by banks.

With this in mind, the aim of this Policy Analysis Paper is to describe the changing ACH landscape, and to consider the degree to which this growth and change have heightened one risk issue in particular: the susceptibility of ACH payments to fraud. The paper is organized as follows. The first section outlines the basic nature of an ACH transaction and describes recent trends in ACH usage. Section II examines basic economic incentives for the growth of ACH transactions. Section III describes significant changes in the nature of ACH payments, focusing in particular on e-checks. Section IV explains how, with the emergence of new ACH applications and the proliferation of third-party processors, the ACH system has become more susceptible to fraud. Section V outlines recent industry and government responses to the growing susceptibility to fraud, and section VI concludes.

I. ACH Basics and Growth Trends

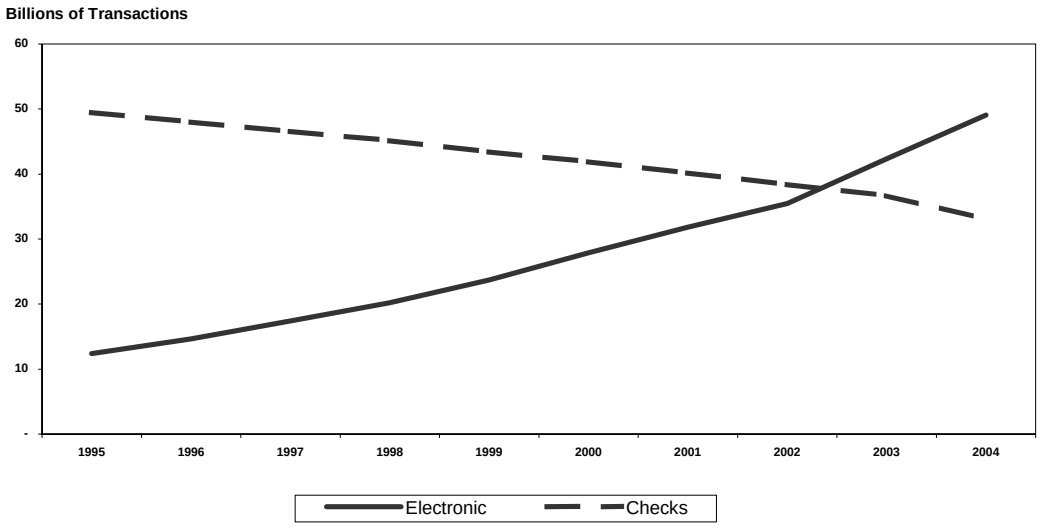
The ACH system is a funds transfer system typically used for retail payments, and was originally developed in the 1970s to provide an alternative to paper checks.[1] It is a batch processing, "store-and-forward" electronic system; that is, transactions received by a bank are stored and processed at a later time, rather than being processed individually. The five participants involved in an ACH transaction are the payor, the payee, the payor's bank, the payee's bank, and the

[1] Analysts and practitioners divide payments into "wholesale" and "retail" payments. Wholesale payments consist of large-value electronic funds transfers such as wire transfers (Fedwire and CHIPS) used for time-critical payments, and interbank settlement. Retail payments include the majority of domestic payments made by consumers, businesses, and governments. The major components of retail payments in the United States include cash, checks, credit cards, debit cards, and ACH transactions. Unlike the other forms of retail payments, reliable records for the number and value of cash payments are not compiled, and hence exact data on cash usage is impossible to obtain. In this paper the term "payments" covers noncash retail payments only.

provider of the ACH service between the two banks. ACH transactions can be either credits or debits. A credit transaction is initiated by the payor: for example, direct deposit of payroll is originated by the employer through the employer's bank, which transfers money to the employee's bank account. A debit transaction is originated by the payee: for example, a mortgage payment is originated by the lender through the lender's bank, which initiates the payment transferring funds from the customer's bank account. Increasingly, a sixth set of participants, third-party processors, has become a significant presence in the ACH system. Third-party processors handle aspects of the origination of ACH payments, and as such insert themselves into the payment process between a payor and the payor's bank (for ACH credit transactions), or between the payee and the payee's bank (for ACH debit transactions).

Broadly speaking, ACH transactions, along with credit card and debit card transactions, comprise retail "electronic payments." In the United States, retail payments historically had been dominated by paper checks, but very recently the volume of electronic payments surpassed payments by check, as illustrated in Figure 1. Prior to 1995, electronic payments grew steadily, but so did check usage, albeit at a declining rate. However, since 1995, electronic payments have displaced check usage to an extent large enough to result in an absolute decline in the number of checks.

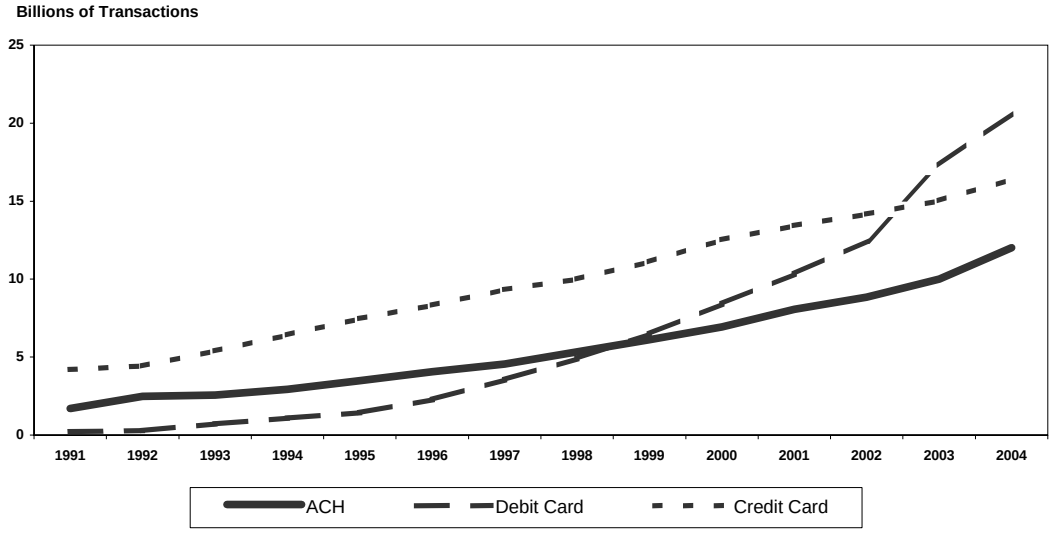
Figure 1. Electronic Payments Overtake Checks



Source: Office of the Comptroller of the Currency using data from *Statistics on payment systems in selected countries* , Bank for International Settlements (various issues); *The Nilson Report* (various issues); and *ATM & Debit News* (various issues). Check volume for 2004 is an estimate.

Increased use of ACH payments contributed to the overall growth of electronic payments (and, by extension, the decline in check usage), but, as Figure 2 illustrates, the substantial and steady growth of ACH payments was exceeded by the growth rate of credit card usage and, especially since 1999, the surge in debit card use. Nevertheless, in dollar-value terms, ACH transactions dwarf card transactions, and have increased substantially both absolutely and, as Figure 3 illustrates, relative to all electronic and check retail transactions.

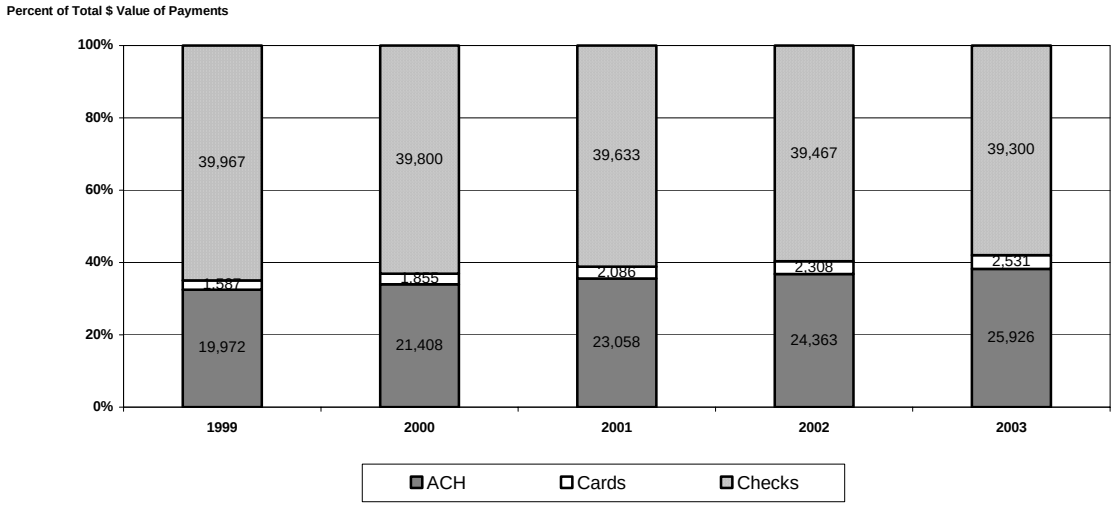
Figure 2. Growth in Electronic Payments



Source: Office of the Comptroller of the Currency using information from *The Nilson Report* (various issues); *ATM & Debit News* (various issues); and NACHA.

Figure 3. Relative Importance of ACH Grows in Value Terms

(Figures within bars in billions of $)



Source: Office of the Comptroller of the Currency using data from *Statistics on payment systems in selected countries*, Bank for International Settlements (various issues).

II. ACH Benefits for Banks, Businesses, Government, and Consumers

Growth in the use of ACH transactions can be explained by two basic factors. The first is the significant benefits depository institutions ("banks"), businesses, government, and consumers derive from this form of payment. This section describes the nature of these advantages. The second impetus for growth in ACH transactions is the emergence of new ACH applications, a subject discussed in the next section of the paper.

II.A. ACH Benefits for Banks

The Federal Reserve is a major processor of payments by check and by ACH, and payments processing costs facing the Federal Reserve can be considered at least broadly illustrative of underlying payments-processing costs for financial institutions.[2] Figure 4 illustrates the widening processing cost advantage for ACH transactions versus checks for the Fed. In 1995, per transaction processing costs for each type of payment were equal, at 3.5 cents per item. Over the next decade, processing costs for paper checks rose to 5.1 cents per item. Meanwhile, technological improvements, deregulation of the communications industry, and increasing economies of scale in ACH transactions processing resulted in a greater than two-thirds decline in per item processing costs, to just under 1 cent, making it one-fifth as costly to process an ACH payment versus a payment by paper check.[3]

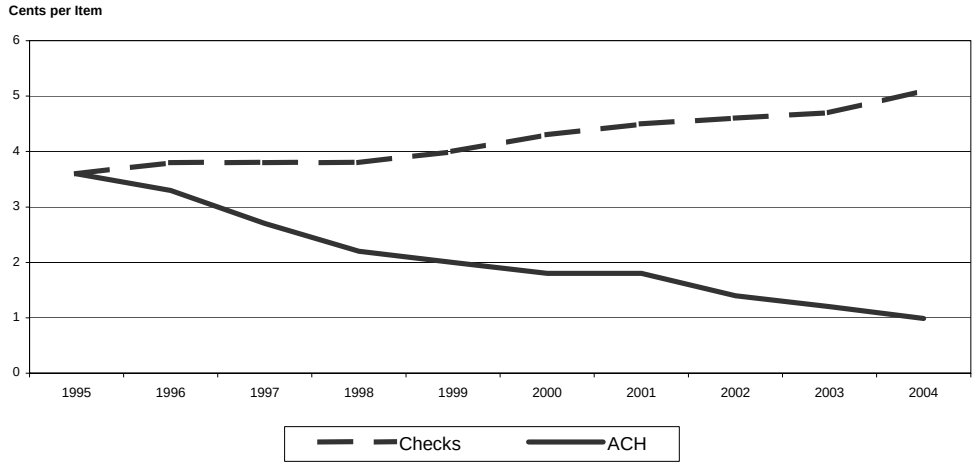
[2] Check and ACH payments are also processed by private clearinghouses and "on us" (i.e., within a bank which is the same for the payor and the payee). In 2003, the latest year for which comprehensive data is available, the Federal Reserve processed 44 percent of all checks and 66 percent of all ACH transactions. See the Committee on Payment and Settlement Systems (2005, Table 7, p. 159). In order that private sector payment processors not be faced with an "unfair" competitive disadvantage compared to the Federal Reserve, the Monetary Control Act of 1980 requires the Federal Reserve to price its payments processing services such that it is able to cover the costs of providing these services.

There is some debate in the payments industry over Federal Reserve System ACH pricing policy. For example, in a December 2002 whitepaper, The Electronic Payments Network (EPN), the only remaining private sector ACH operator, questioned whether the main goal of the Federal Reserve's pricing policy was ACH processing costs recovery, or preservation of market share, especially in light of the Federal Reserve's rapid ACH price reductions in 2001 and 2002. The EPN whitepaper noted that the Reserve Banks did not expect to recover the full costs for all priced services (and, indeed, the Federal Reserve has not recovered 100 percent of the cost of priced services since 2000). EPN also notes that a few months after the first two Fed ACH price reductions, the American Clearing House announced that it could no longer compete in the new price environment. Early in 2005, the Board of Governors requested comments on possible changes to the private-sector adjustment factor (i.e., the method used to compute a target return-on-equity). Periodically, the Board reviews its methodology for calculating this factor in order to determine if, in light of changing business and regulatory conditions and practices, the methodology is still appropriate.

[3] Federal Reserve System, *Annual Report* (various issues). The existence of large-scale economies in the processing of electronic payments is well established. Bauer and Ferrier (1996) estimated scale economies in the Federal Reserve's ACH processing such that a 10 percent increase in ACH volume was associated with only a 4.8 percent increase in processing expenses.

Figure 4. Processing Cost Advantage for ACH Increases

(Costs for the Federal Reserve)



Source: NACHA, using data from the Federal Reserve System.

Payment-processing cost changes have been passed along to banks. In recent Congressional testimony, a Federal Reserve payment system official noted that "Over the past decade, the reductions in the processing costs for ACH have allowed Reserve Banks to cut approximately in half the fees they charge depository institutions for providing ACH services. Over the same period, the Reserve Banks have increased the price of their more labor-intensive paper check service approximately 50 percent."[4] As a consequence, one large bank estimated that it cost about $0.08 to $0.10 to process a check, compared to $0.02 to $0.04 to process an ACH payment.[5]

II.B. ACH Benefits for Business and Government

Cost advantages also accrue to businesses and government from using ACH payments. First, there is a long-standing awareness in the business and government communities of the benefits of ACH direct deposit of payroll. The National Automated Clearing House Association (NACHA), an industry group of ACH network participants, estimates that a typical large company switching from the cutting and distribution of paper paychecks to ACH direct deposit of payroll might realize per transaction savings of $0.187. With a payroll of, for example, 100,000 transactions per month, annual cost savings would amount to $224,400. Even a small business with, say, 500 payroll transactions per month, could cut costs by $0.352 per payroll

[4] Testimony of Louise L. Roseman, Director, Division of Reserve Bank Operations and Payment System on *Recent developments in the payments system*, before the Subcommittee on Financial Institutions and Consumer Credit, Committee on Financial Services, U.S. House of Representatives, (April 20, 2005).

[5] Schneider, Ivan, "JPMC Prepares for Check Conversion Growth," *Bank Systems & Technology* (May 11, 2004).

transaction, saving perhaps a few thousand dollars per year by switching to ACH direct deposit of payroll.[6]

A second advantage businesses have increasingly pursued is the use of ACH transactions for customers' bill payments. As an example, BellSouth Corp reports ACH as the least expensive form of electronic payment for bills. It costs the utility around $2.00 when a customer pays a phone bill with a credit card, and $0.50 to $0.60 for PIN debit, compared to only $0.10 to $0.15 for an ACH payment.[7]

A third, relatively recent source of ACH benefits is in check conversion at the lockbox using the ACH system.[8] Illustrative of the magnitude of savings in this respect are credit card issuers' check conversion savings. In particular, credit card issuers have reported that checks converted to ACH transactions at a lockbox resulted in operational cost savings of $0.057 per consumer check converted. Based on this per item savings, credit card issuers collectively saved an estimated $99.6 million in 2004.[9] Additionally, converting a check to an ACH transaction can reduce card issuers' losses due to the shorter return timeframes for ACH items compared to checks.[10]

Governmental entities disperse millions of payments annually, and ACH transactions convey significant advantages. For example, in its 2004 Annual Report, the Federal Reserve reported figures for check and ACH processing costs for services provided to the federal government: $24.25 million to process 234 million government checks at 10.4 cents apiece, and $5.35 million to process 940 million government ACH payments at 0.57 cents per item. Hence, for the federal government, paying by check was almost 20 times more costly than paying by ACH.[11]

---

[6] There is a difference in the per item savings between the hypothetical large and small companies because the NACHA estimates include some differences in account services and significant differences in the pricing structure for banking services for the two businesses.

[7] Kuykendall, Lavonne, "Chase Offers Payments Consulting to Billers," *American Banker*, June 3, 2005.

[8] Such an ACH transaction is called an "accounts receivable conversion" or "ARC" transaction. See Box 1 for a detailed description of ARC transactions.

[9] Nelson, Bill, "Inside the Numbers – How Costs/Benefits Impact the Growth of ACH Payments, " *Electronic Payments Journal*, Volume 3, Issue 7 (November/December 2004) estimates that the credit card industry accounted for 78 percent of the 2.24 billion commercial ARC and WEB originations. ARC and WEB are ACH transactions used as substitutes for check payments; they are described in detail in Box 1, below.

[10] Converting checks to ACH has a greater impact on the processing of returned deposited checks than on the forward collection of checks. This is because, for example, the largest banks (the banks most likely to be handling lockbox processing for a credit card issuer) receive funds on the majority of checks deposited (90 percent of local checks and 63 percent of non-local checks) within one business day. However, the average time for the return of deposited checks is often longer than the return time for ACH items. See the ABA Deposit Account Survey Report (2004) for information on average check processing and return cycle times.

[11] 91st Annual Report, Board of Governors of the Federal Reserve System (2004), pp. 125-126.

II.C. ACH Benefits for Consumers

Consumers have also found substantial savings of time and effort, as well as added security, by choosing direct deposit of paychecks compared to receiving a paper paycheck. The popularity of this form of ACH payment is reflected in the fact that 75 percent of Social Security recipients sign up for direct deposit when they register for benefits.[12]

Consumers' familiarity with direct payroll deposit likely increases their penchant for adopting other forms of ACH payments. For example, using sample results from two surveys, Klee and Hayachi (2003) constructed a model to predict the probability that a user of direct deposit would use direct bill payment.[13] They found that the use of direct deposit by a person represents a 21 to 24-percentage point increase in the predicted likelihood of that person adopting direct bill payment. In a related vein, Klee and Hayachi found that consumers who use new technology products (e.g., the Internet) are more likely to use electronic forms of payment than those who do not. Others have observed the emergence of a strong correlation between growth in the adoption of broadband (high-speed) Internet connectivity and growth in online banking, and some expect the growth of broadband access and online banking to propel online bill payment. [14]

As of December 2004, there were approximately 36 million U.S. households using online banking – more than a fivefold increase from the seven million online banking households in December of 1998.[15] Although growth in the number of net new households adopting online banking slowed to nine percent in 2004, the increase in Internet banking customers at one large bank was considerably higher.[16] Bank of America has the largest online banking customer base with a reported 13.8 million active online banking customers – an increase of 38 percent for the 16 months ending in August of 2004.[17] During the same time period, the number of Bank of America customers using online bill payment increased by 68 percent. Consistent with the broadband-online banking correlation noted above, Bank of America found that more than 60 percent of its customers used high-speed Internet connections for online banking. The rapid growth in the adoption of online bill payment at Bank of America and other banks may, in part, account for the recent increase in the rate of growth for "customer initiated entries" (CIE), a type

---

[12] Jackson, Ben, "Treasury to Tout Direct Deposit of Social Security," *American Banker*, August 2, 2005.

[13] Hayashi, Fumiko, and Elizabeth Klee, "Technology Adoption and Consumer Payments: Evidence from Survey Data," *Review of Network Economics*, Vol. 2, Issue 2 (June 2003).

[14] On the first point see "Big Broadband Buy-In Feeds On-Line Banking," *Bank Technology News*, Vol.18, No.7, page 17, (July 2005), and McGrath, James C., "Will Online Bill Payment Spell the Demise of Paper Checks?" *Payment Cards Center Discussion Paper*, Federal Reserve Bank of Philadelphia (July 2005). McGrath also comments on the second point.

[15] *Online Banking Report*, Number 114 (January 17, 2005).

[16] *Ibid.*

[17] Press Release (August 16, 2005) "Bank of America wins awards for best consumer Internet bank and best information security initiatives," and Press Release (April 21, 2004) "Growth propels Bank of America to 10 million subscriber milestone."

of ACH credit transaction. Based on second quarter 2005 volume, CIE entries will increase an estimated 40 percent this year, compared to an increase of 14 percent in 2004.

III. The Changing Nature of ACH Transactions: New Applications

In addition to strong growth for traditional ACH transactions such as those for recurring consumer payments, a new set of ACH debit transactions, termed by some as "electronic checks" or "e-checks," have spurred overall ACH growth. (See Box 1 below). E-checks differ in

Box 1. ACH "E-Checks"

- A Point-of-Purchase (Standard Entry Class code "**POP**") entry is created for an in-person purchase of goods or services when, for example, a merchant receiving a paper check from a consumer uses it as a source document to electronically enter its routing number, account number, serial number, and dollar amount of the transaction into a point-of-sale terminal or other electronic system to generate a debit entry to the consumer's demand deposit account. The merchant obtains a written authorization from the consumer, and the paper check is voided and returned to the consumer at the point-of-purchase. POP payments are "nonrecurring" or "single-entry" (one-time) in the sense that even if, for example, a consumer's grocery store always uses this method when the consumer presents a check to pay for weekly grocery purchases, each transaction must be authorized anew by the consumer at the point-of-sale. POP is an example of "check conversion."

- An Accounts Receivable Conversion ("**ARC**") entry also uses the consumer's check as a source document, but not at the point-of-sale. Rather, the routing number, account number, check serial number, and dollar amount of the transaction are captured using a scanning device and converted to an electronic ACH entry after a biller receives the consumer's check in the mail, or at a lockbox location for payment of goods and services. ARC transactions can be "recurring" in the everyday sense of the word, in that a consumer's monthly paper check payment to a credit card company may routinely be processed as an ARC transaction. However, such payments are not recurring and pre-authorized in the same sense as would be the case if a consumer arranged for his credit card company to automatically debit his bank account in order to pay the bill every month.

- A Telephone-Initiated ("**TEL**") entry is created when a consumer gives authorization via the telephone for her account to be debited electronically by the party the she wishes to pay. This type of entry may only be originated when there is either an existing relationship between the consumer and the payee or, if there is no pre-existing relationship, only when the consumer has initiated the telephone call. TEL transactions are single-entry; that is, a separate oral authorization must be obtained for each debit.

- An Internet-Initiated ("**WEB**") entry is created when a consumer authorizes a merchant or other payee, via the Internet, to debit the consumer's account. In contrast to other forms of e-checks, WEB payments can be used for pre-authorized transactions, as for example when a consumer "signs" with an electronic signature via the Internet an agreement for recurring automatic debits to his account for repayment of a loan. However, many WEB transactions are single-entry. These single-entry WEB transactions may be with a merchant or other originator new to the consumer, or the consumer may have an established relationship with an originator, as for example when a consumer authorizes the payment of his credit card bill online at the credit card issuer's website.

important respects from preauthorized and recurring ACH payments.[18] With traditional, recurring ACH transactions, after an initial set of payment instructions is successfully processed, payments are repeated using the same routing and account number details, thus limiting the likelihood of errors.[19]

E-checks are a recent advance in ACH payments. POP came into use in September 2000, while the other three applications began in 2001 or 2002. Adoption of e-checks grew rapidly however, and e-checks now account for over 40 percent of all ACH debits, compared to 6 percent in 2001. Figure 5 shows the changing composition, both absolute and relative, of the four components of e-checks over the recent past. ARC, which did not exist until 2002, had by the end of 2004 become the dominant form of e-checks, with 941.7 million transactions accounting for 47 percent of all e-checks.[20] WEB usage also grew steeply over this period, from 54 million transactions in 2001, to 715 million in 2004. TEL transactions, though less in total volume than either ARC or WEB, nevertheless grew from 6.3 million to 187.7 million, a thirty-fold increase over the four-year period. Even POP almost tripled between 2001 and 2004, from 64.2 million to 162.3 million transactions (although POP was the only e-check application to experience single digit growth in 2004).[21] Of note, although ARC has come to dominate e-check payments, most industry observers believe that its dominance will be transitory because as the decline in check-writing gains further momentum, conversion of checks via ARC will taper off correspondingly.[22]

[18] It is important to distinguish e-checks from "check electronification." Check electronification refers to a process to speed up check processing, most commonly by "check truncation," which essentially means to stop, or hold, the paper, and subsequently process electronically the information contained on the check.

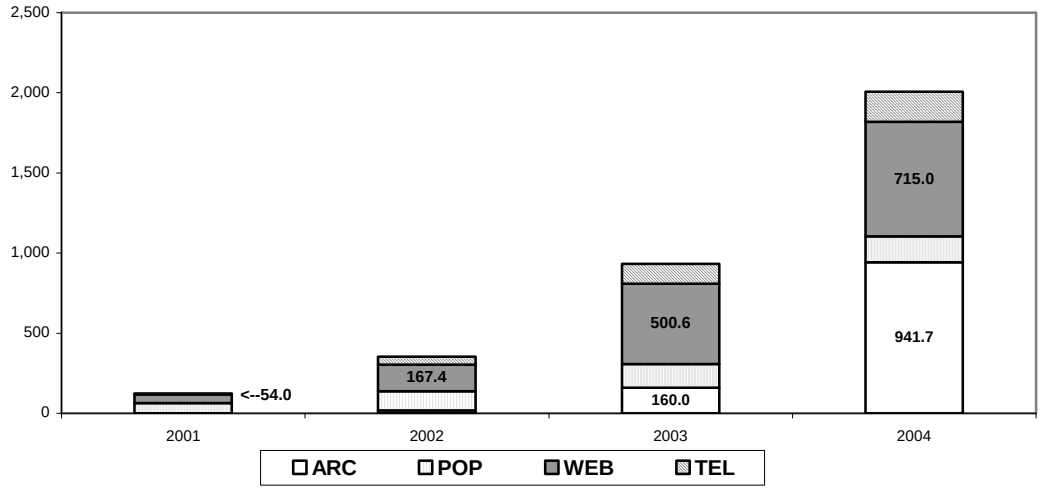
[19] If there is a change in the bank's routing number, or in the consumer's account number, the bank will send a "notification of change" ACH entry.

[20] The figures used here are for network volume and exclude on-us items. Including on-us items 2004 ARC volume was 1.3 billion. A few originators could account for a large portion of ARC transactions, which may help to explain ARC's rapid growth. For example, if a single credit card issuer such as Citibank adopted ARC and converted around 60 percent of all monthly payments received for active accounts, this one "adopter" of ARC could generate over one third of all ARC transactions originated in 2004. Citibank has more active accounts than other card issuers, but a handful of large credit card issuers could account for most of the ARC transactions. Credit card issuers account for around 78 percent of ARC and WEB transactions.

[21] These figures exclude on-us transactions.

[22] Some payments research firms expect ARC to top out at about 3.5 or 4 billion transactions around 2007 or 2008, and decline substantially thereafter. Others expect ARC to level off and decline slowly as fewer paper checks are used to pay bills. See *American Banker* (July 1, 2005), and Hoffman, Karen Epper, "Payment's Mass Conversion," *Banking Strategies*, Volume LXXXI Number II, (March/April 2005).

Figure 5. ACH: Growth and Changing Composition of E-Checks
(Millions of Transactions)



Source: Office of the Comptroller of the Currency using data from NACHA. Excludes on-us transactions.

IV. ACH Transactions: Susceptibility to Fraud

The growing use of new ACH applications is a clear indication that ACH network participants are finding increasing value in them. Nevertheless, some of these new applications have increased the susceptibility of the ACH system to fraudulent transactions. This section deals first with certain characteristics of ACH e-checks that may raise their susceptibility to fraudulent use. No ACH payments, including e-checks, are subject to real-time authorization of "good funds." Until recently, that potential vulnerability was of limited concern because ACH payor and payee generally enjoyed an ongoing payment relationship. However, with the emergence of e-checks, the lack of a recurring payment relationship between the payor and payee coupled in some cases with the lack of a physical "source" document, have raised fraud vulnerability.

The second part of this section points out that there are also long-standing characteristics of the ACH system that make it vulnerable to fraud. These include weak fraud detection and prevention mechanisms, weaknesses in the incentive structure for return items, and weak system governance mechanisms. In general, when ACH transactions are pre-authorized and recurring between a consumer and an originator who are known to each other, these ACH system vulnerabilities present a low risk of fraud; but as the last part of this section explains, the addition of new ACH applications has attracted new participants, creating new opportunities for fraudsters. These fraudsters have exploited some of the new ACH applications for which an established customer-originator relationship is not necessarily a requirement.

Ahead of a more detailed discussion of the ACH system's susceptibility to fraud, it is important to bear in mind that banks experience relatively fewer ACH fraud losses versus check fraud

losses, a point Table 1 helps to illustrate. Smaller size banks in particular are less likely to have experienced ACH fraud losses compared to check fraud losses. However, large banks, which are more intensely involved in ACH transactions than small banks, also experience lower ACH fraud loss than check fraud loss. In this respect, ACH transactions have had a relatively good track record.

Table 1. Bank Fraud Losses: Checks vs. ACH
(2003)

	Bank Size Groups (in Assets)			
	Under $500 million	$500 million to $4.99 billion	$5 billion to $49.99 billion	$50 billion or more
Percent of Banks with Fraud Losses:				
Check-related	72	97	100	100
ACH-related	23	40	61	72
Median $-Value of Fraud Loss:				
Check-related	$5,042	$51,353	$977,508	$8,716,014
ACH-related	$250	$3,543	not available	not available

Source: ABA Deposit Account Fraud Survey Report (2004)

IV.A. Susceptibility to Fraud: New ACH Applications

Fraudulent (i.e., "unauthorized") payments within the ACH system have always been costly to deal with as "return" items, but because of ongoing payment relationships that characterize traditional ACH transactions, incidence of fraud was historically very low.[23] Most e-checks, on the other hand, do not involve preauthorization for a series of recurring payments. In addition, some e-checks are "spontaneous" in nature – that is, there is no pre-existing payment relationship between consumer and payee.[24] Because consumer and payee may have little or no knowledge of each other's veracity, the probability of payment fraud is higher, and therefore the risk of costly return items is higher. However, the different types of e-checks differ in their relative vulnerability to fraud.

[23] A "return" item is returned to the originating bank because the originating bank warrants that all transactions it originates into the network are authorized. If a debit is returned as "unauthorized" this means that a consumer has notified his bank (the payor's bank) that the transaction was not authorized. Another reason for return items is error (i.e., incorrect information). Two primary sources of incorrect information are 1) the consumer gives inaccurate information during the enrollment process, or 2) the information related to the consumer or the consumer's account at the payor's bank changes, such as when a once-valid routing number changes after a bank merger, or a once-valid account number changes because a consumer closes an account but opens another account at the same bank.

[24] The four e-check transactions (ARC, POP, TEL and WEB – described in Box 1) are consumer applications (i.e., they are meant to be used to originate debit entries to a consumer's account).

In general (and in the absence of counterfeit checks), ARC and POP payments, e-check applications that use a paper check as a source document, are less vulnerable to fraud than TEL and WEB payments, which are conducted remotely and do not use a paper check as a source document. Although numerous variables affect riskiness, ARC, which is currently the least risky ACH debit application, is likely to remain a low-risk application because of the way it is used (i.e., to pay recurring bills such as loan payments and utility bills). Under current conditions, the unauthorized payments rate for POP transactions is similar to that for traditional preauthorized debits (i.e., PPD payments).[25] However, the risks associated with POP mirror the risks associated with accepting paper checks in a retail environment.[26] As more "good" payments migrate away from checks to electronic payment instruments such as credit and debit cards, and as fraudsters continue to concentrate on payment instruments that do not provide real-time transaction authorization – such as checks – the rate of check fraud is likely to increase. In tandem with this development, there could be an increase in the proportion of fraudulent checks presented at the point-of-sale that are then converted to ACH transactions. WEB transactions, executed via the Internet, are subject to that medium's fraud vulnerabilities, but NACHA requirements for WEB transactions, and the fact that the majority of WEB transactions are being used for bill payment transactions between a consumer and an originator who are known to each other tend to reduce the risk profile of this e-check application.[27] Because TEL shares the weaknesses of WEB but lacks the features that tend to mitigate fraud vulnerability, it is likely to remain a higher risk ACH application.

IV.B. Susceptibility to Fraud: ACH System Characteristics

Fraud Detection and Prevention Mechanisms. Vulnerabilities in ACH fraud detection and prevention mechanisms can best be understood in comparison with contrasting features of credit and/or debit card systems.[28] First, unlike in the case of credit card transactions, the ACH system has no system-wide method to link a payor's name, address, and deposit account number. Second, the ACH system has no mechanism for real-time authorization of transactions, as is the

[25] NACHA data for 2004 show that the unauthorized return rate for POP was 0.05 percent, slightly lower than the 0.07 percent rate for PPD.

[26] Note that the allocation of liability among the parties to a transaction is different between checks and ACH payments, because different laws and regulations cover these two forms of payment. This in turn may change the degree of risk assumed by the payee and/or the payee's bank in an ACH transaction compared to a check transaction.

[27] The NACHA Rules impose heightened security requirements for WEB transactions and direct originating banks to establish procedures to monitor the credit-worthiness of originators of WEB transactions on an on-going basis, thus requiring banks to investigate merchants and to have an understanding of their business and financial condition.

[28] It is of course important to keep in mind that per item costs for processing credit and debit card transactions are considerably higher than for ACH transactions in part because of these differences. Credit card networks provide services that are valued by merchants, including card authorization, verification and payment guarantees. Among other things, these services reduce the risk of fraud and facilitate risk management. For an analysis and empirical evaluation of the benefits to merchants provided by credit and debit card networks, and the related network investments, see Guerin-Calvert, Margaret and Janusz A. Ordover, "Merchant Benefits and Public Policy Towards Interchange: An Economic Assessment," Presented at Federal Reserve Bank of New York conference on *Antitrust Activity in Card-Based Payment Systems: Causes and Consequences* (September 2005).

case with, for example, credit cards. Third, the ACH system lacks the kind of measures credit card systems have for fraud detection.[29] In particular, credit card issuers have long incorporated procedures for "vertical" fraud detection – identifying a pattern of seemingly anomalous transactions for a particular account. In addition, and more importantly from a systemic perspective, card systems employ procedures for "horizontal" fraud detection. Such measures can identify cases when, for example, there is a large volume of payments for the identical amount across the system, as might occur if criminals were attempting large-scale fraudulent debit transactions after stealing customer account numbers from a merchant. The absence of these measures make it easier for fraudsters to exploit the ACH system and to avoid detection.

Incentive Structure for Return Items. Maintaining the traditionally low incidence of return items associated with the ACH network is important in order to maintain confidence in the system. In addition, return items place a relatively high burden on some system participants. First, on a per-item basis, ACH returns are costly. Based on a survey of banks, NACHA estimated that the cost to the payor's bank for handling an ACH return is between $12 and $17 per item.[30] Second, procedures for dealing with return items greatly disadvantage banks receiving unauthorized or fraudulent ACH debits to consumer accounts.[31] In particular, the payor's bank earns no direct fee or income to offset the receipt of consumer ACH debits, and it has to bear the cost of the return process, including the cost of obtaining a written statement from its account holder victimized by the unauthorized transaction.[32] Under such circumstances, the continued growth of both traditional and new ACH payments is likely to increase the return-item processing costs for some banks.

In addition to the high per-incident costs for return items, growth in return items is likely to exacerbate potentially unsafe and unsound incentives embedded in the ACH returns system. In particular, fee income from return items can become an important source of non-interest income for an originating bank. Even if an ACH transaction originator (i.e., the payee) has an unusually high level of returns, from a fee perspective the bank for whom that originator is a client has a disincentive to deny or even limit ACH origination services, because the bank earns a fee from the originator on both the initial presentment of the (faulty) debit entry, as well as the return.

[29] Although no ACH network-wide solutions currently exist, payments industry participants are aware of these problems and some partial solutions exist. For example, using the data in debit bureau files, providers of databases used for opening bank accounts and for check verification and guarantee services can help validate some ACH transactions. Merchants are most likely to use this type of service when converting checks to ACH payments at the point of sale (i.e., POP). Section V further discusses industry responses.

[30] "Network Return Entry Fees Questions and Answers," *Electronic Payments Journal*, Volume 3, Issue 7 (November/December 2004). As the article points out, this cost does not include potential indirect costs such as closed accounts and reputation damage.

[31] Note that NACHA Rules require the payor's bank to accept all ACH entries it receives.

[32] In an effort to address problems with the current price structure, NACHA and its Board of Directors proposed a Network Return Entry Fee ("NREF") to provide an incentive to originating banks to prevent unauthorized payments from entering the ACH network, and to compensate the payor's bank for the costs associated with processing ACH items returned as unauthorized. The NREF would shift the financial responsibility from the payor's bank to the payee's bank (i.e., the originating bank). Though a majority of NACHA members voted for the May 2005 ballot initiative, the proposed change did not achieve the necessary two-thirds vote to become effective.

Additionally, and unlike in the case of check-processing, a bank originating ACH debit transactions is not constrained by the necessity of having to maintain demand deposit accounts with every originator. Under these circumstances, some banks may not scrutinize returns at the originator level, increasing the likelihood that they will continue to process transactions for acquired merchants with high return rates operating through one or more third-party processors.

ACH System Governance Mechanisms. Vulnerabilities in the ACH system's fraud detection and prevention mechanisms, and incentives in the return-items pricing structure that may (unintentionally) reward some originating banks for practicing inadequate due diligence on questionable originators could be counter-balanced by an effective governance system. A key element to such a system is the existence of a central authority with power to effectively monitor and, if necessary, expel participants whose actions undermine the ACH system's integrity.[33] In the Visa and American Express card systems for example, Visa and American Express function both as system operators and as governing bodies for their respective networks. This arrangement enhances their ability to monitor system participants. In addition, the major credit card and debit card systems have the ability to ban merchants who have excessive charge-backs.[34] For most merchants, the threat of being expelled from participation in the card networks appears to serve as an effective deterrent. By contrast, for the ACH system, NACHA is primarily a rules-setting body without the same operational control and ability to monitor members' compliance, or to expel members who consistently participate in the origination of a high rate of return items.

IV.C. Susceptibility to Fraud: New System Participants

As pointed out, the level of ACH fraud traditionally has been relatively low, especially in comparison to check fraud rates, even in the presence of the vulnerabilities just discussed. However, with the proliferation of new participants in the ACH system, especially in combination with the increase in the volume of ACH payments, industry observers have begun to worry about the rising number of unauthorized returns and opportunities for fraudulent exploitation of system vulnerabilities.[35]

[33] While this type of central authority can facilitate risk management, it does not eliminate risk. Recent security breaches at several major merchants (e.g., B.J.'s Wholesale Club, DSW Shoe Warehouse, etc.) and the processor CardSystems have led some industry observers to question how many processors and merchants are not complying with the payment card industry's data security protocol.

[34] Generally, before a merchant account is shut down, penalties are imposed and, depending on the severity of the chargeback levels, a correction plan may be agreed to between the merchant, the acquiring bank, and the card association. Card networks, like the ACH system, are faced with an increase in the number and types of merchants participating in their networks. Representatives from Visa and MasterCard met in September of 2005 to discuss requiring more rigorous security audits to address these changes.

[35] See for example *News from FedACH*, Vol. 1, No. 1, Retail Payments Office, Federal Reserve Bank of Atlanta (Q4 2003), and Vol. 1, No. 5 (Q4 2004).

Technological advancements have reduced scale and information-processing barriers to entry into the payments system for third-party service providers, including third-party processors.[36] As a result, the number and relative importance of third-party processors has increased along with the growth of the ACH network. A third-party processor is an entity that acts in an intermediary ACH transaction-processing capacity between an originator and an originating bank.[37] For example, a third-party processor could be a traditional data-processing service bureau, or an independent sales organization that specializes in acquiring merchants engaged in high-risk transactions (e.g., mail order and telephone merchants).

In the course of providing services to ACH originators, these third party processors become both customers of originating banks and intermediaries between banks and originators. It is possible that such "layering" between a bank and an originator might diminish or eliminate the due diligence a bank would otherwise perform were it to have a direct customer relationship with the originator. Where third-party processors contract with independent sales organizations or other third-party processors, there may be two or more layers between banks and originators. Problems tend to arise when neither the third-party processor nor the originating bank performs due diligence on the companies for whom they are originating payments.[38] This becomes increasingly important as new third-party processors specializing in lower volume, but higher margin transactions enter the ACH network; such participants are more likely to violate the rules of the ACH network (i.e., the NACHA Rules) or generate illegal transactions. Without adequate monitoring at the originator level, layering makes it easier for illicit originators to operate undetected.

An originating bank is responsible for all the entries it submits into the ACH network regardless of the extent to which one or more third-party processors may have been involved. Third-party processors are, in general, not subject to the same level of regulation and supervision as banks; under similar circumstances, payment card networks have devised procedures to help identify the third-parties involved in the system, promoting a measure of industry-imposed governance over the operations of third-party participants.[39] The ACH network lacks a comparable system-wide identification process. As the ranks of nonbank third-party participants in the ACH system

[36] We use the term "third-party processor" for a subset of third-party service providers referred to in the NACHA Rules as "third-party senders." The fraud risk issues raised in this paper are related to this subset of third-party processors. Other third-parties perform tasks outsourced to them by originating or receiving banks and/or have direct access to an ACH operator. Risk issues related to such third-party service providers are beyond the scope of this paper.

[37] For ACH debits, an originator is the payee, i.e., the entity to whom funds are paid.

[38] Fox, Jeannette, "NACHA on mitigating risk in the ACH network," *Fedfocus: News from the Federal Reserve Banks,* Volume 3, Issue 2, Federal Reserve Financial Services (April 2005); and *News from FedACH*, Vol. 1, No. 1, Retail Payments Office, Federal Reserve Bank of Atlanta (Q4 2003)

[39] For example, in addition to bank sponsorship, third parties must also be registered with Visa. Although registration is required, John Shaughnessy, Visa USA's Senior Vice President, Fraud Prevention, recently noted that they are "seeing a lot of unregistered agents in the system." Forward Financial Bank Card Conference, Memphis, Tennessee (September 2005).

swell, especially in response to opportunities arising from new payment applications, the lack of such industry-imposed governance procedures increase the risk of fraud.

Given these circumstances, ACH industry observers have expressed concerns about fraud, especially for two of the newer ACH transaction types, TEL and WEB.[40] There is evidence to justify these concerns, as Table 2 illustrates. In particular, Table 2 shows that in 2002, nearly 1 percent of TEL transactions, and significantly more than half a percent of WEB transactions were "unauthorized" – i.e., cases where a consumer's account was debited but the consumer asserts that he did not authorize the transaction. Those rates were substantially higher than

Table 2. Unauthorized TEL & WEB Returns
(percent of total transactions, by type of ACH payment)

	2002	**2003**	**2004**
TEL	0.86	0.19	0.21
WEB	0.68	0.47	0.08
Prearranged Payment (PPD)	0.10	0.09	0.07

Source: NACHA.

traditional pre-authorized ACH debits. Indeed, though both unauthorized transactions rates for TEL and WEB declined after 2002, unauthorized TEL transactions rates were still three times the rate for traditional preauthorized ("PPD") debits. As explained in the next section, industry efforts to avert fraudulent ACH efforts have played a role in the decline in unauthorized payments rates for TEL and WEB. Nevertheless, fraudsters still appear to be taking advantage of TEL transactions.

V. Susceptibility to Fraud: Industry and Government Responses

Amid a growing recognition that new ACH users and uses have heightened fraud vulnerabilities, industry participants and government authorities have introduced measures to combat rising fraud rates. Industry and government responses have focused primarily on measures to stop "bad actors" from entering the system to begin with, and on measures to monitor ACH activities in order to make it more difficult for illicit parties to continue processing ACH payments if they nevertheless manage to enter the system. The common theme for most recent industry and government measures is better due diligence by participants with respect to their direct customers, as well as the "customers of their customers." In effect, these measures counteract existing vulnerabilities in the system's fraud detection and prevention mechanisms. Indirectly, they also address system governance issues by encouraging each participant to take more individual responsibility for policing bad actors.

[40] See in particular the interview with Richard Oliver, Senior Vice President, Retail Payments Office of the Federal Reserve Bank of Atlanta, in *News from Fed ACH*, Vol. 1, No. 5, Retail Payments Office, Federal Reserve Bank of Atlanta (December 2004).

V.A. Industry Responses

As Table 2 illustrated, there is a significantly higher unauthorized transactions rate for TEL than for other types of ACH debits, and as a consequence recent industry (and government) responses have focused on this form of ACH payment in particular. Industry participants have observed that the return problem is a result of several factors, most notably banks originating payments without performing adequate due diligence on companies for whom they originate payments, and telemarketers skirting the NACHA Rules or engaging in deceptive or in some cases illegal practices.

NACHA has observed a strong correlation between high unauthorized return rates and originators (i.e., merchants) who are violating the NACHA Operating Rules, and who are engaged in fraudulent or deceptive marketing practices. In order to help identify potential fraud within the ACH network, NACHA receives data from the Federal Reserve and EPN (the two ACH operators) on the volume of return entries sent back to originating banks. NACHA uses this data to identify originating banks with unusually high returns volume, and alerts the originating bank if it believes that bank should review an originator's activity and compliance with the NACHA Rules. Because merchants involved in fraudulent or deceptive practices typically experience higher than average rates of unauthorized returns, NACHA has adopted a rule requiring originating banks to provide it with information about the merchant, the nature of the merchant's business, and the merchant's explanation for the excessive unauthorized TEL return rates above 2.5 percent. The monitoring of excessive returns by NACHA and EPN has led to a significant reduction in the rate of unauthorized returns. As shown previously in Table 2, the rate of unauthorized TEL returns in 2004 (0.21 percent) was less than one-fourth the rate of returns in 2002 (0.86 percent).

NACHA has also implemented rule changes and worked with industry participants to improve the quality of WEB transactions. Partly as a consequence, the 2004 rate for unauthorized WEB returns was one-eighth the 2002 rate.[41] More generally, payees are using bank debit less often than in prior years as a method of payment for transactions associated with telemarketing fraud. Twenty-six percent of fraudulent telemarketing transactions in 2004 were funded with bank debit, down from 37 percent in 2003.[42]

The two ACH operators are also responding to changes in the ACH network. In response to the growing threat of fraud, several years ago EPN developed EPNWatch®, a service that offers

[41] As mentioned in the previous section, the current lower return rates for WEB are also likely due to how the majority of WEB transactions are being used – for bill payment transactions between a consumer and an originator who are known to each other. A three-day random sampling of WEB transactions revealed that 80 percent of these transactions are being used for bill payments, 19 percent for funds transfers, and only one percent for spontaneous purchases. Presentation given by Jane Larimer of NACHA at the FFIEC Payments System Risk Conference, May 10-13, 2005.

[42] "Bank debit" is comprised of demand drafts – paper checks that are produced without a payor signature but which are presumed to have been authorized by the payor – as well as ACH. Information on the use of debits is from the National Consumers League's National Fraud Information Center report *Telemarketing Scams: January – December 2004*.

reports to originating banks when unauthorized payments exceed established thresholds. The reports are designed to alert originating banks to customers with excessive unauthorized returns. The Federal Reserve is pilot-testing a similar service for originating banks, and plans to offer reports as a priced service (in the form of a per-originator fee) starting early in 2006. In addition to its reporting service for originating banks, EPN has announced that it is in the process of developing a report for receiving banks to help them identify fraudulent payments before they are settled.[43]

V.B. Government Responses

Governmental agencies have also responded to fraudulent ACH activities stemming from changes in payments applications and the nature of industry participants. In particular, federal and state government actions have targeted deceptive and fraudulent telemarketing activities in part by taking action against third-party processors and banks that have facilitated such activities by providing access to the ACH system.

An example at the federal level is the complaint filed in January of 2004 by the Federal Trade Commission (FTC) charging a third-party ACH processor, First American Payment Processing, Inc. ("First American") with violating the Telemarketing Sales Rule (TSR).[44] Specifically, the FTC alleged that First American processed ACH payments for telemarketers who they knew or should have known were deceptively selling advance-fee credit cards and engaging in other deceptive or abusive telemarketing practices.[45] Additionally, the FTC alleged that First American engaged in an unfair practice by systematically breaching its contractual promise to banks to adhere to the NACHA Rules governing the ACH network. The NACHA Rules specifically prohibit the processing of ACH transactions on behalf of merchants engaged in "cold-call" outbound telemarketing.[46] The final order issued by the FTC prohibits First American from processing payments if it has information indicating that the business practices of a merchant violate the TSR, NACHA Rules, or the FTC Act.[47] Such information would include when unauthorized return rates exceed the 2.5 percent threshold for return entry monitoring under NACHA Rules, or when there are significant numbers of consumer complaints in any

[43] Wade, Will, "Fed, EPN Develop Tools to Detect, Report ACH Fraud," *American Banker*, April 15, 2005.

[44] See FTC Press Release, February 11, 2004, "FTC Sues Electronic Payment Processor for Facilitating Fraudulent Telemarketing Schemes." In this case the FTC took action against a third party processor that aided telemarketers engaged in illegal practices. Under the TSR, a company can be held liable not only if its own activities are in violation of the TSR, but also if it provides substantial assistance or facilitates a violation of the rule.

[45] The TSR defines an advance-fee loan as an abusive telemarketing practice "requesting or receiving payment of any fee or consideration in advance of obtaining a loan or other extension of credit when the seller or telemarketer has guaranteed or represented a high likelihood of success in obtaining or arranging a loan or other extension of credit." See 16 C.F.R. Section 310.3 (a) (4).

[46] Telemarketing also includes calls generated from advertisements or other solicitations to purchase products or services (i.e., in-bound calls).

[47] Section 5 of the Federal Trade Commission Act (FTC Act), 15 USC 45(a)(1), prohibits "unfair or deceptive acts or practices in or affecting commerce," a model followed by most states. For additional information, see OCC Advisory Letter 2002-3.

given month regarding unauthorized charges. In addition, the order requires First American to investigate the business practices of each of the companies for which it processes transactions.

At the state level, a number of actions have similarly targeted third-party processors that were providing ACH payment services to businesses involved in fraudulent telemarketing schemes.[48] In addition, and very recently, state government officials have underlined banks' responsibilities in thwarting fraudulent ACH activities. For example, in July 2005, the Iowa Attorney General's office entered into an agreement with a community bank in South Dakota that was used by third party processors to gain access to the ACH network.[49] In the Iowa Attorney General's view, the law requires banks not to assist any telemarketer which the bank knows or should have known is engaged in fraudulent conduct.[50] This approach enables the Attorney General's office to combat telemarketing fraud by looking at the businesses providing support to telemarketing schemes, not just the telemarketers directly engaged in fraudulent activity.

Very recent action by the state of Vermont provides additional definition to the scope of ACH system participants' anti-fraud responsibilities. A new law in Vermont, which became effective on July 1, 2005, and which is reported to be the first of its kind in the country, prohibits telemarketers from using the ACH network to transfer funds from a consumer's bank account in connection with any outbound telemarketing, unless the consumer has purchased something from that telemarketer in the past year, or currently has a written agreement with the telemarketer.[51] Additionally, third party processors will be held liable for processing ACH debits or demand drafts for telemarketers that would be illegal if the telemarketers themselves initiated the debit. In the event the telemarketer is "out of reach" (e.g., in another country) or has disappeared, the third party processor will be responsible for compensating victims of the telemarketer. The Vermont law also addresses the telemarketer's bank, which is deemed to be aiding and abetting a fraudulent telemarketer when the bank knows, or consciously avoids knowing, the telemarketer is engaging in an unfair or deceptive act or practice.

Finally, amid changes in payment applications and participants, the bank regulatory agencies have heightened their attention to ACH risk issues. The March 2004 Federal Financial Institutions Examinations Council handbook on retail payment systems specifically cautions banks offering TEL origination services on behalf of their customers to adopt appropriate risk management practices, and warns them that they are exposing themselves to substantial risk if they originate payments for merchants engaged in fraudulent or deceptive business practices.[52]

---

[48]See, for example, *Iowa Attorney General Press Release* (February 15, 2005) "Electracash, Inc. Agrees to Stop Processing Withdrawals for Telemarketing Scams."

[49] The Iowa Attorney General worked with the offices of the Minnesota and South Dakota Attorneys General. These Attorneys General initially contacted the bank in 2002 in the course of investigating the complaints of telemarketing fraud victims. See *Iowa Attorney General Press Release* (July 6, 2005) "First Premier Bank Agrees to Deny Automatic Withdrawal Services to Telemarketing Scams."

[50] Most of the telemarketers involved in the advance-fee credit card scams in the Iowa case processed payments through an intermediary third party, and many of the fraudulent telemarketers used the same third party processor.

[51] See *Press Release, Office of the Vermont Attorney General* (April 5, 2005) "Telemarketing Bill Signed into Law."

[52] FFIEC *IT Handbook*, "Retail Payment Systems," March 2004.

In the same vein, in its December 2004 *Automated Clearing House* bulletin, the OCC encourages banks to focus adequate due diligence efforts on ACH payments originators which are not direct customers of the bank, but are rather customers of third-party processors with which the bank deals.[53] The guidance instructs banks to have controls in place to restrict or refuse ACH services to potential originators engaged in questionable or deceptive business practices.

Additionally, the Comptroller's Handbook on merchant processing informs banks of the need for a formal merchant underwriting and approval policy. This policy should designate the types of merchants with which the bank is willing to do business and the types of merchants with which the bank should refuse to do business (i.e., "prohibited merchants").[54] The Handbook also outlines some of the essential elements of an underwriting policy, such as a background check on merchants to verify the validity of the business.

VI. Summary and Conclusions

This paper began by describing overall trends in ACH payments, and factors underlying the growing demand for ACH payments by banks, businesses, government, and consumers. Its focus then turned to the emergence and rapid recent growth of new ACH payment applications that, unlike traditional ACH debits, do not rely on established customer-originator relationships. Some of these new ACH debit payments in particular have drawn more third-party processors into the ACH system, as well as new merchants eager to use (i.e., originate) the new ACH debits. Most new participants are of course drawn by the opportunities for greater (legitimate) economic benefits, but certain characteristics of the ACH system, especially in tandem with some of the new ACH debit applications, have presented opportunities for fraudsters.

Three long-standing characteristics of the ACH system make it somewhat vulnerable to fraud, although historically fraud rates have been quite low. These vulnerabilities include weak fraud detection and prevention mechanisms, weaknesses in the incentive structure for return items, and weak system governance. Recently, entrance of a new set of ACH system participants – third-party service providers – have increased the complexity of the ACH system by adding one or more layers of participants between originating banks and the entities for whom those banks ultimately are originating ACH payments. This layering heightens the challenge for banks to perform adequate due diligence on originators (i.e., performing adequate "merchant underwriting") – especially those originators which are not direct customers of the bank. Such due diligence is increasingly important because of the opportunities for unscrupulous merchants to engage in deceptive and fraudulent practices, subsequently generating fraudulent payments. Telemarketing has proven to be an especially attractive avenue for such merchants to originate fraudulent debits.

In response to heightened fraud vulnerabilities, industry and government authorities have introduced measures designed to prevent "bad actors" from entering the system, and to make it more difficult for those which do slip through the cracks to continue to exploit the ACH network. The common theme is better due diligence by participants with respect to their direct customers,

[53] Office of the Comptroller of the Currency, *Automated Clearing House*, Bulletin 2004-58, December 20, 2004.

[54] *Merchant Processing*, Comptroller's Handbook (December 2001).

as well as the "customers of their customers," measures aimed specifically at counteracting existing vulnerabilities in the system's fraud detection and prevention mechanisms.

As the ACH system continues to adapt to the changing needs of its users, banks in particular will be subject to increased risk management challenges, including the misuse and fraud that has followed an increase in the volume and changes in the production of ACH payments. Bank supervisors need to ensure that banks choosing to be in the business of originating ACH entries understand the new challenges, and have an adequate risk management program and board and management oversight.