An Examination of Remotely Created Checks

By Ana R. Cavazos-Wright[1]

The paper is intended for informational purposes and the views expressed in this paper are those of the author and do not necessarily reflect those of the Federal Reserve Bank of Atlanta or the Federal Reserve System.

I. Introduction

Almost everyone, whether recently or in years past, has authorized the initiation of a draft transaction from a checking account, whether to expedite a payment to a creditor, to purchase an item via telephone or Internet, or agree to compensate a merchant for the return of an initial paper check due to insufficient funds. Bill payment systems generate draft transactions against checking accounts to help reduce consumer chargebacks in cases of new users with limited credit history or for large value items.[2] Likewise, collections agencies and mutual funds initiate draft transactions from checking accounts to establish payment plans.[3]

Each of these transactions involve the origination of remotely created checks, and as the terms imply, they are checks created 'remotely' by a payee, under the authority of the account holder, but do not bear the account holder's signature.[4] Remotely created checks are similar to their check counterparts in that they embody a paper instrument that contains an unconditional written order, instructing a drawee bank (paying bank) to make payment to the order of a designated payee[5] and are processed through the banking system. Yet, unlike traditional checks,

[1] Ana R. Cavazos-Wright is a payments risk analyst in the Retail Payments Risk Forum. Ana is grateful to Clifford S. Stanford, assistant vice president and former director of the Retail Payments Risk Forum and Crystal D. Carroll, former senior payments risk analyst in the Retail Payments Risk Forum, for their initial drafting of this paper and extensive research committed to this subject matter.

[2] George F. Thomas, *It's Time to Dump Demand Drafts*, Digital Transactions News, July 2008, at 40.

[3] Comments of the National Consumer Law Center on behalf of its Low-Income Clients and Consumer Federation of America Consumers Union National Association of Consumer Advocates U.S. Public Interest Research Groups to Proposed Amendment to Regulation J and CC Regarding Remotely Created Checks, May 11, 2005, at 5 [hereinafter Comments of the NCLC], available at: http://www.consumerlaw.org/initiatives/test_and_comm/content/RCCommentsFed5.pdf.

[4] Regulation CC, 12 C.F.R. § 229.2(fff) (2007).

[5] U.C.C. § 3-104(f) (2006).

the payee, and not the account holder, creates the instrument that instructs the drawee bank to make payment.[6]

Unfortunately, the inherent ease with which a remote payee can create remotely created checks is also the reason why these payment instruments have drawn scrutiny.[7] On the surface, they appear to be subject to a higher likelihood of abuse because the collection of a remotely created check does not require or rely upon a signature or any other documentation to indicate authorization, and an unauthorized remotely created check can be generated in an automated fashion, even using common desktop tools[8]. The publicized large-scale incidents of fraud[9], Canada's prohibition[10], and outcries from some encouraging the United States to follow Canada's lead[11], has postured remotely created checks center stage as a controversy within the world of negotiable instruments. Notwithstanding the controversy, remotely created checks continue to be a legally legitimate payment method. Supporters say they serve a valid commercial role by providing account holders with faster and simpler payments that go beyond one-time ACH debit transactions.[12]

This paper explores the unique attributes of remotely created checks, how these attributes shaped legal reform, the risk management challenges they present, and which industry stakeholder is best poised to manage these challenges.

---

[6] Supra note 4.

[7] See, e.g., Charles Duhigg, *Bilking the Elderly, With a Corporate Assist*, N.Y. Times, May 20, 2007, A1 (available at: http://www.nytimes.com/2007/05/20/business/20tele.html); Letter from Representative Edward J. Markey and Congressman Barney Frank, to The Honorable John M. Reich, Director, Office of Thrift Supervision, June 11, 2007 [hereinafter Letter from Markey and Frank], available at: http://financialservices.house.gov/press110/061107_markey_frank_letter_unsigned_checks.pdf) (citing the N.Y. Times May 20, 2007 story).

[8] For example, the use of specialized software and printers enable payees to create a paper version of the check that was authorized over the phone or Internet. See Comments of the NCLC, supra note 3, at 2.

[9] See, e.g., supra note 7; Letter from Lynne M. Ross, Executive Director, National Association of Attorneys General, to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System, May 9, 2005, at 2-5 [hereinafter Letter from National Association of Attorneys General] (on file with author).

[10] There is no rule explicitly prohibiting tele-cheques in Canada, rather it is the Canadian Payments Association's (CPA) policy to prohibit their use. See CPA, June 1, 2003, announcing "Prohibition of Tele-cheques in the Clearing & Settlement System" effective January 1, 2004, available at http://www.cdnpay.ca/news/tele.asp. See, also CPA rule "(h) A Telecheque may be returned for the reason "Not Eligible for Clearing" up to and including 90 calendar days after being received by the Drawee", available at http://www.cdnpay.ca/rules/pdfs_rules/rule_a4.pdf.

[11] See, e.g., Letter from National Association of Attorneys General, supra note 9, at 2-5; Comments of the NCLC, supra note 3, at 2.

[12] See, e.g., Letter from Jeffery P. Neubert, President & C.E.O., The Clearing House, to Jennifer J. Johnson, Secretary, Board of Governors of the Fed. Reserve System, May 3, 2005, at 5-6 [hereinafter Letter from The Clearing House] available at: http://www.nych.org/reference/comment_letters/2005cl/000731.pdf .

II. Remotely Created Checks Generally

A remotely created check[13] is defined under Regulation CC (Reg. CC)[14], as amended in 2005 by the Federal Reserve Board, as:

> . . . [A] check that is not created by the paying bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn. For purposes of this definition, "account" means an account as defined in paragraph (a) of this section as well as a credit or other arrangement that allows a person to draw checks that are payable by, through, or at a bank.[15]

In its simplest form, the issue or creation of a remotely created check is a matter between the account holder (drawer) and payee. The drawer grants the payee (merchant) authorization[16] to produce a remotely created check drawn on the drawer's account. The payee obtains the information that appears in the MICR[17] line of the drawer's physical checks, and based on this information, the payee enters the check information and creates either an electronic template of a check or sometimes a paper check document that looks like a check. The check does not bear the drawer's signature; instead the signature line displays the drawer's name or some other verbiage referencing the drawer's authorization to create the check.[18]

The payee may create the remotely created check or use a third party processor to create, print, and deposit the remotely created check into accounts held by either the payee or the processor serving as agent of the payee at the depository bank.[19] The item once created is sent forward for collection through the banking system in the same manner as a traditional check, i.e., to a collecting bank (such as a Federal Reserve Bank), and presented for payment to the drawer's

---

[13] Also known as: preauthorized draft, demand draft, telecheck, paper draft, or RCC.

[14] In amending Reg. CC, the Federal Reserve Board also proposed conforming cross-references to the new warranties in Regulation J, see Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire and Availability of Funds and Collections of Checks, 70 Fed. Reg. 10,509 (proposed March 4, 2005) (codified at 12 C.F.R. §§ 210, 229) [hereinafter Proposed Reg. CC Rule].

[15] Supra note 4 (commentary states that this definition does not apply to checks where the drawer's signature is forged).

[16] An authorizing party can be a consumer, corporation, unincorporated company, partnership, government unit or instrumentality, trust, or any other entity or organization. § 229.2(fff)(3).

[17] MICR means Magnetic Ink Character Recognition, which are the numbers at the bottom of a paper check, printed in magnetic ink, that can be read by machines indicating the name and address of the drawee financial institution, account number, check number, and when the check is cleared, the dollar amount of the check is added. § 229.2(vv); Dictionary of Banking Terms (5th ed. 2006).

[18] Regulation CC, 12 C.F.R. § 229 (2007), 70 Fed. Reg. 71,218.

[19] Id. at 71,218 – 71,219.

bank (payor bank).[20] The payor bank debits the drawer's account and credits the depository bank, who in turn credits the payee's account.[21]

Like traditional checks, remotely created checks can also be processed electronically by converting the paper check into an electronic file that is acceptable to image-exchange networks.[22] But, unlike a traditional check, which is signed in paper form by the drawer before the check is image captured and converted into an "electronic item,"[23] an electronic remotely created check (one never printed) can still be presented for payment using an electronic template, and nevertheless be sent forward for clearing in a format indistinguishable from files of images captured from paper checks. The payee still obtains the requisite account information and purported authorization from the account holder, but in this instance, a paper check is never presented for processing.[24] Instead, an electronic image of a check is created, bearing a legend referencing authorization by the account holder.[25] Typically, a payee contracts with a third party processing company[26] to create the electronic remotely created check.

In recent years, the use of these "electronic remotely created checks" has increased. The primary reason is to avoid the costs of printing and to leverage off the imaged-based processing permitted under the Check Clearing for the 21st Century Act[27] (Check 21). Yet, no matter their form (paper or electronic), it is possible for these payment orders to wind up converted and processed as an ACH debit item and cleared through the ACH network.[28]

Whether processed through the check collection system or ACH network, remotely created checks' most common uses include: (1) pre-authorized drafts, where for example, a consumer approves a payment of its insurance policy and the company issues an unsigned draft

---

[20] Proposed Reg. CC Rule, supra note 14, at 10,511.
[21] Id.
[22] See, e.g., Regulation J, 12 C.F.R. § 210.2 (defining "item" in section 210.2(i) to include "electronic item," such as an "electronic image of a check or any other paper item").
[23] Infra note 83.
[24] Letter from The Clearing House, supra note 12, at 5-6; see also UCC § 4-110 (electronic presentment of checks).
[25] Id.
[26] For example: AE Checking, CheckSavers, Landmark Clearing, and MyECheck. *Editor's note: the Federal Reserve does not endorse any third party product or service, and these companies are listed as examples only to illustrate the point.*
[27] 12 U.S.C. §§ 5001-5018 (establishes the ability of financial institutions to use substitute checks created from check images).
[28] FFIEC Retail Payments Booklet 2010, at A-31-A-32, available at: http://www.ffiec.gov/ffiecinfobase/booklets/Retail/retail.pdf. However, remotely created checks are ineligible for ACH conversion under NACHA Operating Rules.

for the amount; (2) ACH administrative returns, where the ACH item is returned because the information originally provided from the MICR line cannot be properly processed and the merchant resubmits the ACH item as an unsigned draft; (3) telephone purchases, typically, where telemarketers call selling products or services to companies or individuals, and the telemarketer requests information from the consumer about its bank account for the purposes of obtaining payment; (4) depository transfer checks, instances where companies initiate transfer payments between their accounts, some of which may be between different banks; (5) return item fees, created by merchants to cover fees for returned checks; and (6) bill payment, where the consumer authorizes a creditor such as a credit card company to create a remotely created check in order to timely pay a bill that would otherwise be late if paid with a traditional paper check.[29]

Even though remotely created checks are used for a variety of legitimate commercial purposes, and by a variety of players in the payments industry, opponents of remotely created checks advocate for their abolition, explaining that remotely created checks do not generate sufficient value or convenience today to outweigh the risks and costs that result from the fraudulent use of remotely created checks.[30]

Examples of Remotely Created Check Fraud

In recent years, incidents of remotely created check fraud shed some light on the unique risks they present. The following are examples of those widely publicized incidents and the steps taken by regulators and law enforcement agencies against those directly and indirectly involved, while pursuing redress for those victimized by the fraud. The first is FTC v. 3rd Union Card Services Inc.[31] According to the FTC, the alleged scheme began as early as 2004 when the defendants, going by the name "Pharmacycards.com," electronically debited, in increments of

[29] Letter from The Clearing House, supra note 12, at 5-6.; see also Letter from The Electronic Check Clearing House Organization to Jennifer J. Johnson, Secretary Board of Governors of the Federal Reserve System re: Comments to Proposed Amendments to Regulation CC, May 2, 2005, at 9, [hereinafter Letter from ECCHO] available at: http://www.eccho.org/documents/RegCCRCC.pdf.

[30] Thomas, supra note 2, at 40; see also Letter from National Association of Attorneys General, supra note 9, at 6; but c.f., 12 C.F.R. § 229 (general comments to final rule state that additional research is required about the use of remotely created checks and the commercial impact an outright ban would have on the industry before justifying prohibition by statute or regulation).

[31] Civil Action No.: CV-S-04-0712-RCJ-RJJ, available at: http://www.ftc.gov/os/caselist/pharmacycards/pharmacycards.shtm.

$139, as many as 90,000 consumers' accounts without their knowledge or consent.[32] The defendants attempted to fraudulently debit more than $10 million from consumers' checking accounts in less than three months by accessing bulk bank account information through multiple third party payment processors and creating remotely created checks and ACH transactions.[33] The fraudsters were able to abscond with almost $900,000 in ill-gotten gains and would have made an additional $2 million had their assets not been frozen.[34] Ultimately, the FTC filed suit and won a default judgment against Pharmacycards.com for $5.3 million.[35]

Law enforcement agencies also pursued third party processors since often times they serve as middlemen for fraudsters seeking to obtain consumers' financial data from banks.[36] In the Pharmacycards.com case the FTC filed a separate action against InterBill, a third party processor that acted as a gateway into the banking system for Pharmacycards.com.[37] Allegedly, InterBill created remotely created checks and deposited those checks into an account held in InterBill's name at a Wells Fargo bank for the benefit of Pharmacycards.com.[38] The FTC alleged that InterBill failed to perform appropriate due diligence in its relationship with Pharmacycards.com or follow its own risk management guidelines for new merchants, even after observing return rates as high as 70 percent.[39] A federal court agreed, and ordered a judgment against InterBill for $1.7 million.[40]

---

[32] News Release: FTC Halts Unauthorized Bank Charges in Bogus Pharmacy Card Scam (May 27, 2004) (available at: http://www.ftc.gov/opa/2004/05/pharmcards.shtm)

[33] Id.

[34] FTC v. 3rd Union Card Services, Memorandum of Points and Authorities in Support of Plaintiff's Application for a Temporary Restraining Order (TRO) and Order to Show Cause Why a Preliminary Injunction Should Not Issue, May 21, 2004, available at: http://www.ftc.gov/os/caselist/pharmacycards/040521pharmacycardtropanda.pdf (FTC's Motion for TRO with Asset Freeze and Other Equitable Relief granted on May 25, 2004, available at: http://www.ftc.gov/os/caselist/pharmacycards/040525pharmacycardstro.pdf).

[35] FTC v. 3rd Union Card Services, Default Judgment and Order for Permanent Injunction and for Monetary Relief granted on July 15, 2008, available at: http://www.ftc.gov/os/caselist/pharmacycards/050719pcjdmtorder.pdf.

[36] Supra note 31; see, e.g., On January 26, 2010, a class action suit was filed against five national banks and three third party processing companies for their participation in an alleged fraudulent telemarketing scheme, available at: http://www.courthousenews.com/2010/01/29/TelemarketPhilly.pdf.

[37] News Release: FTC Sues Payment Processor That Took Millions From Consumers' Accounts Without Their Knowledge (January 8, 2007) (available at: http://www.ftc.gov/opa/2007/01/interbill.shtm). In 2005, the FTC also sued Universal Processing, another company that processed payments for Pharmacycards.com, see: http://www.ftc.gov/os/caselist/0423190/0423190.shtm.

[38] FTC v. InterBill, Ltd and Thomas Wells, Complaint for Injunction and Other Equitable Relief, December 26, 2006, available at: http://www.ftc.gov/os/caselist/0423192/070108cmp0423192.pdf.

[39] Id.

[40] FTC v. InterBill, Ltd. and Thomas Wells, Final Judgment and Order for Permanent Injunction and Other Equitable Relief, April 30, 2009, available at: http://www.ftc.gov/os/caselist/0423192/090618interbillfo.pdf.

In another instance, the United States Attorney's Office for the Eastern District of Pennsylvania brought a civil action against Payment Processing Center, LLC (PPC), for allegedly processing consumer payments for an international network of fraudulent telemarketers.[41] The alleged scheme was described as:

> [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 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.[42]

The federal court entered a permanent injunction against the processing company which meant a lifetime ban against PPC, its owners and managers, from ever engaging in any activity where unsigned checks are used to process payments for telemarketers.[43] PPC was forced to liquidate its assets, and from those funds a multi-million dollar restitution fund was created for those victimized by the fraud.[44]

In April 2008, Wachovia bank, who served as the bank of first deposit for various third party payment processors and telemarketers[45], including Payment Processing Center, LLC, faced an enforcement action by the Office of the Comptroller of the Currency (OCC) for "unsafe and unsound" practices in the improper oversight of deposit accounts held by telemarketers and PPC.[46] The OCC alleged that Wachovia, through its inadequate due diligence over its customer relationships, shared responsibility with the payment processors and telemarketers that perpetrated payments fraud against thousands of individuals through the use of remotely created

---

[41] New Release: District Court Enters Permanent Injunction Against Payment Processing Center, February 12, 2007, available at: http://www.justice.gov/usao/pae/News/Pr/2007/feb/PPC.html.
[42] Id.
[43] New Release: District Court Enters Permanent Injunction Against Payment Processing Center, February 12, 2007, available at: http://www.justice.gov/usao/pae/News/Pr/2007/feb/PPC.html.
[44] Id.
[45] The payment processors and telemarketers involved: Payment Processing Center, LLC; FTN Promotions, Inc. dba Suntasis, Inc.; Netchex Corp.; and Your Money Access LLC, and related companies. News Release: OCC, Wachovia Enter Revised Agreement to Reimburse Consumers Directly, December 11, 2008, available at: http://www.occ.treas.gov/ftp/release/2008-143.htm.
[46] News Release: OCC Directs Wachovia to Make Restitution to Consumers Harmed by the Bank's Relationships with Telemarketers and Payment Processors, April 25, 2008, available at: http://www.occ.treas.gov/ftp/release/2008-48.htm.

checks.[47] According to the OCC, Telemarketers obtained consumers' account information over the phone and then the telemarketer or payment processor would create a remotely created check and deposit the funds into a Wachovia bank account.[48]

Following an eighteen-month investigation, the OCC determined that Wachovia management should have been alerted to the potentially fraudulent business practices of PCC and the telemarketers through the high rate of return of remotely created checks.[49] Ultimately, the OCC and Wachovia reached a settlement agreement, whereby Wachovia, while admitting no fault, agreed to make restitution to all who were victimized by PCC and the telemarketers (estimated maximum amount of potential claims of $125 million), forfeit the fees it earned through its banking relationship with PPC and telemarketers (approximately $8.9 million),[50] contribute those funds to consumer education programs particularly for the elderly, and pay approximately $10 million in civil money penalties.[51] In total, Wachovia agreed to pay over $140 million.[52]

The 2008 Wachovia settlement with the OCC sent an important message to banks about the need for stronger oversight programs for the inherent risk associated with certain payment relationships.[53] The settlement, whether intended or not, raised more questions than answers for banks trying to calibrate risk management decisions.[54] This case was precedent-setting. Going forward every bank must now consider its potential responsibility and financial liability for financial losses that result from the bad behavior of its bank customers or customers' customers, specifically, the fact pattern where that bad behavior takes the form of defrauding third party victims and using the bank's services to obtain payment from those defrauded victims.[55] From

---

[47] Id.
[48] Id.
[49] Id. (In some instances, remotely created checks returned to Wachovia exceeded 50 percent of the total deposited, even so, management did not terminate these account relationships or do anything else to correct the problem). Agreement by and between Wachovia Bank and The Treasury Comptroller of the Currency, #2008-028, April 24, 2008.
[50] Id. (Wachovia earned $3.9 million in related fee income from its accounts with PCC and telemarketers).
[51] Id.
[52] Id.
[53] Richard M. Fraher, Assistant General Counsel, Federal Reserve Bank of Atlanta, *OCC v. Wachovia . . . How will this ground-breaking enforcement action change the landscape for banks, regulators, law enforcement, and consumers?*, slide #7, #9 (on file with author).
[54] Id. at slide #9.
[55] Id. at slide #10; see also News Release: OCC and T Bank Enter Agreement to Reimburse Consumers, April 19, 2010 (T Bank agreed to pay over $105 million in restitution and civil money penalty for their relationships with a

the bank's perspective, the most important question about the liability principle established by the Wachovia enforcement action may be, what would define the potential scope of such exposure?[56] On the other hand, from a consumer's perspective, the focus after the Wachovia enforcement action may be whether the remedies in the Wachovia case went far enough to ensure that the victims were adequately compensated.[57]

III. Laws and Legal Reforms Addressing Remotely Created Checks

In recognition of the inherent differences between remotely created checks and traditional paper checks, regulatory and legal reforms were established in response to the unique risks introduced by remotely created checks. For instance, the Federal Trade Commission (FTC) has in place the Telemarketing Sales Rule (TSR)[58], which prohibits specific deceptive and abusive telemarketing acts or practices.[59] FTC views telemarketing as fraudsters' favored method for fleecing consumers' bank accounts through the use of remotely created checks.[60] In shaping the TSR to mitigate the risk of remotely created check fraud, the FTC included provisions in the rule that require the telemarketer to obtain consumers' express verifiable authorization to use bank account information for the purposes of obtaining payment.[61] Consistent with FTC regulations, NACHA[62] also requires a consumer's readily identifiable authorization to use bank account

---

third party payment processor involving the use of remotely created checks), available at: http://www.occ.treas.gov/ftp/release/2010-45.htm.

[56] Id. at slide #9

[57] On December 11, 2008, the OCC entered into a revised settlement with Wachovia that directed the bank to issue checks to consumers that may have been harmed by payment processors or telemarketers that had account relationships with Wachovia. http://www.occ.treas.gov/ftp/release/2008-143.htm. The settlement was challenged as inadequate by three members of Congress and others as *amici*. See Motion and Brief of Representatives Barney Frank, Eward Markey and Joseph Sestak, in support of the Intervenor *Faloney* Plantiff's Motion for an Injunction Under the All Writs Act, *USA v. Payment Processing Center, LLC* (E.D. Pa. May 29, 2008).

[58] 16 C.F.R § 310.

[59] Id. (requires telemarketers to make specific disclosures of material information; prohibits misrepresentations; prohibits calls to consumers who have asked not to be called again, and sets payment restrictions for the sale of certain goods and services).

[60] Prepared Statement of the Federal Trade Commission Presented by Jodie Bernstein Director of the Bureau of Consumer Protection "Demand Draft Fraud" Before the House Banking Committee Washington, D.C. April 15, 1996 [hereinafter Statement by Bernstein] (FTC estimates that remotely created check fraud has caused millions of dollars in consumer injury), available at: http://www.ftc.gov/speeches/other/ddraft.shtm.

[61] Id.

[62] NACHA (National Automated Clearing House Association) is a non-profit association that develops operating rules and business practices for the Automated Clearing House (ACH) Network and for electronic payments. http://www.nacha.org/c/intronacha.cfm.

information for a one-time ACH debit. However NACHA's rules are less prescriptive as far as what an 'identifiable authorization' looks like.[63]

The FTC ensured that the TSR's reach extended beyond telemarketers by also including individuals and organizations that are not in the telemarketing business, but who generate and process remotely created checks for those who do.[64] This kind of business generally acts as a third party processor who takes the bank account information provided by the telemarketer (merchant) and generates a remotely created check.[65] The third party processor then forwards the remotely created check to the merchant for deposit into the merchant's bank account, or the third party processor itself pays the merchant and deposits the item into the processor's bank account.[66] Then, as noted earlier, the remotely created check proceeds through the banking system in the same manner as traditional paper checks.[67]

In 2002, the National Conference of Commissioners on Uniform State Laws and the American Law Institute approved revisions to Articles 3 and 4 of the Uniform Commercial Code (UCC) to address the concerns raised over remotely created checks.[68] Prior to 2002, Articles 3 and 4 of the UCC contained no special provisions for remotely created checks. The revisions defined a remotely created check (but termed it 'remotely-created consumer item') as "an item drawn on a consumer account, which is not created by the paying bank and does not bear a hand written signature purporting to be the signature of the drawer."[69]

Revisions to Articles 3 and 4 also included new transfer and presentment warranties that required the person transferring a remotely created check (remotely created consumer item) to warrant "that the person on whose account the item is drawn authorized the issuance of the item for which the item is drawn."[70] Effectively, UCC's amendments altered the long standing final

[63] NACHA Operating Rule 2.1.8 states in part "the [seller] must either (1) tape record the oral authorization, or (2) provide the [buyer] with written notice confirming the oral authorization", including: the date on or after the ACH entry will settle; the amount of the transaction; customer's name and telephone number customer may call for inquires; and the date of oral authorization. The oral authorization applies only to a single-entry ACH debit.
[64] Statement by Bernstein, supra note 60, at 3.
[65] Id.
[66] Id.
[67] Id.
[68] Proposed Reg. CC Rule, supra note 14, at 10,510.
[69] UCC § 3-103 (a)(16) (2005).
[70] UCC § 3-416(a)(6); *see also* § 4-207(a)(6) (containing almost identical language).

payment rule of *Price v. Neal*[71] and created an incentive for depository banks to supervise their relationships with customers who deposit remotely created checks.[72] Unfortunately, by March 2005, only fourteen states had adopted the UCC's revisions to Articles 3 and 4, and no state had adopted the UCC's revisions in their entirety.[73] Instead, several states enacted their own remotely created check provisions, which varied markedly from the UCC both in scope and form.[74] Such lack of uniformity left the statutory coverage of remotely created checks porous and susceptible to forum shopping by unscrupulous payees.[75]

In an effort to resolve the disparate treatment of remotely created checks among states, the Federal Reserve Board proposed to amend Reg. CC in March 2005. The changes proposed would be similar to the amendments made to Article 3 and 4.[76] The final rule, announced in November 2005, became effective July 1, 2006.[77] In essence, amendments to Reg. CC, like the UCC, but with some variations, reallocated the risk of loss resulting from an unauthorized remotely created check from the paying bank to the depository bank.[78] Furthermore, under the Reg. CC amendments, any bank that transfers or presents a remotely created check warrants that the check is authorized by the person on whose account the check is drawn.[79]

The Board believed that the amendments to Reg. CC would make it easier for a depositor to obtain a refund if an unauthorized remotely created check has been posted to the depositor's account. The new rule would "create an economic incentive for depository banks to perform the requisite due diligence on their [remotely created check] customers."[80] The warranties

---

[71] 97 Eng. Rep. 871 (K.B. 1762) (established that the paying bank must bear the economic loss of an unauthorized check).
[72] UCC § 3-416 cmt. 8 (discussing the limited rejection of the *Price v. Neal* rule and the appropriateness of shifting the burden to the depository bank for ensuring remotely created checks are properly authorized).
[73] Supra note 14, at 10,510 (listed the following 14 states: Arkansas, California, Colorado, Hawaii, Idaho, Minnesota, Nebraska, New Hampshire, North Dakota, Oregon, Tennessee, Texas, Utah, Vermont, West Virginia, and Wisconsin); see also, infra note 75, at 3.
[74] Supra note 14, at 10,510.
[75] Letter from Lance Liebman, Chair, Permanent Editorial Bd. for the U.C.C., to Jennifer J. Johnson, Secretary, Bd. of Governors of the Fed. Reserve Sys. 3, March 11, 2004, at 3, [hereinafter Letter from the UCC] available at: http://www.ali.org/ali_old/PEBComments04.pdf.
[76] See supra note 14, at 10,510-10,511. A year earlier, the Board requested commentary on whether it should amend Reg. CC, and based on overwhelming support, a more detailed proposal resulted in March 2005. See Availability of Funds and Collection of Checks, 69 Fed. Reg. 1470 (proposed Jan. 8, 2004) (codified at 12 C.F.R. § 229).
[77] Regulations J & CC 12 C.F.R. §§ 210 and 229 (2007).
[78] Id.
[79] Id.
[80] Supra note 14, at 10,510.

ultimately shifted liability for the loss created by an unauthorized remotely created check to the bank of first deposit.[81] Transfer and presentment warranties for all other items remain unchanged, i.e., liability is retained by the paying bank.[82] It is also important to note that only banks make the new Reg. CC warranty, which creates only bank-to-bank rights and obligations, and no new rights or obligations are created for depositors.

IV. Events Following Amendments to Regulation CC

In anticipation of warranty claims as a result of amendments to Regulation CC, the Federal Reserve Banks, in their role as check clearing intermediaries, amended Operating Circular No. 3 (OC 3) in July 2008. The changes required the payor bank, asserting a warranty claim on an unauthorized remotely created check through the Federal Reserve System, to submit a sworn statement that the remotely created check was not indeed authorized.[83] The payor bank was required to specifically submit:

> (i) a complete adjustment request in a format prescribed by the Federal Reserve Bank; (ii) a legible copy of the front and back of the check; and (iii) a statement [in a format prescribed by the Federal Reserve Bank] from a person on whose account the check was drawn asserting under oath that issuance of the check was not authorized with regard to either the amount stated on the check, the payee stated on the check, or both.[84]

The amendments to OC 3 exclude electronic remotely created checks, i.e., those remotely created checks that never take the form of paper, from the warranties the Federal Reserve Banks would otherwise make in the normal course of check collections.[85] OC 3 clarified that an item does not constitute an 'electronic item' unless the data captured originally derived from a paper

[81] Press Release, Federal Reserve, Board announces final rule governing remotely created checks (November 21, 2005) (available at: http://www.federalreserve.gov/boarddocs/press/bcreg/2005/20051121/default.htm).
[82] Id.
[83] Board of Governors of the Federal Reserve System, Operating Circular No. 3: Collection of Cash items and Returned Checks, § 20.10, July 2006, [hereinafter OC 3] available at: http://www.frbservices.org/files/regulations/pdf/operating_circular_3.pdf.
[84] Id..
[85] Id.

check.[86] The Federal Reserve Banks reasoned that because these items never existed as paper checks, they were not recognized under check law.[87]

The ability to send electronic remotely created checks, in place of paper, for clearing through Federal Reserve Banks or other check clearing networks, allows vendors to debit a higher volume of checking accounts, including some that cannot be debited through ACH because they are ineligible.[88] Electronic processing allows marketers, payment processors, bill collectors, etc., to turn online payment instructions from consumers into electronic files. In turn, the electronic files are formatted into files acceptable to image-exchange networks, resulting in faster clearing and settlement than what is possible with paper remotely created checks.[89]

Today, third party processing companies openly market their ability to create electronic only remotely created checks.[90] These companies boast an ability to obtain faster deposit and settlement, limit chargebacks, and generate multiple payments (unlike ACH TEL or WEB entries).[91] For example, Landmark Clearing, a third party processing company, states the following on its website:

> "Any company that has 1% Unauthorized Returns or more will need to stop processing ACH and look for other payment methods. For legitimate companies that cannot meet this limit, [our service] is for you."[92]

The business model for most of these companies is predicated on creating electronic remotely created checks to include the information normally found on a paper check as provided to them by their customer and then clearing them through the Check 21 clearing networks.

---

[86] Id. at § 21.0.

[87] An electronic image of a check created by a merchant, usually at the point of sale, is often incorrectly referred to as an 'electronic check,' instead what is created is an ACH debit entry, and governed by Regulation E and not U.C.C. articles 3 and 4. The check itself is not a 'check' under check law, but rather is viewed as a source document providing the needed information to originate an electronic funds transfer. 12 C.F.R § 205.3(c)(1) (2006); See also U.C.C. § 4-110, an item needs to have existed at some point for article 4-110 to apply; See also generally, Press Release, Retail Payments Office of the Federal Reserve System from Rich Oliver to Chief Executive Officers at Depository Institutions (June 16, 2008) [hereinafter Oliver Press Release] (on file with author).

[88] Oliver Press Release, supra note 87.

[89] Id.

[90] For example, MyECheck announced its patent for remotely created checks in accordance with Check 21 specifications. See Wireless News, *MyECheck Receives Patent for Remotely Created Check Service*, June 29, 2008.

[91] This kind of reoccurring payment plan is not permitted under NACHA rules as an ACH debit using the "TEL" or "WEB" codes, because each payment must be authorized separately. For a discussion of TEL entries, see NACHA Operating Guidelines §IV, ch. XVII and ch. XVIII for a discussion of WEB and TEL entries respectively.

[92] Landmark Clearing's statement was referencing NACHA's 2007 network enforcement rules that monitor unauthorized returns exceeding 1 percent of originated items within certain classifications (on file with author).

However, using electronic remotely created checks for ACH ineligible conversion eschews ACH unauthorized return monitoring and control procedures, while bypassing check law entirely. This leaves Reserve Banks or other check clearing networks unable to provide Check 21 warranties, causing them to look to the sending financial institution (bank of first deposit) to recuperate any loss as a result of an unauthorized electronic remotely created check. It is possible, however, that because electronic remotely created checks originate from electronic instructions that they could fall under the requirements of the Electronic Funds Transfer Act (EFTA) and Regulation E, but that determination has not been explicitly made since as a general matter Regulation E does not apply to payments originated by check or other similar paper instruments.[93]

Consequently, OC 3 also added new warranty and indemnification sections where the bank of first deposit warrants that the electronic data submitted for processing qualifies as an 'electronic item,' as described above, and further indemnifies the Federal Reserve Banks from any loss if the data is subsequently determined not to be an electronic item.[94] This means that the bank of first deposit who presents an item that does not qualify as an electronic item will have breached an express warranty and will assume liability for any loss incurred by the Federal Reserve Banks.[95]

V. Risk Management Concerns

The amendments to Reg. CC require banks to give separate risk management consideration to their potential roles as either a paying or depository institution. From the perspective of the paying institution, it is likely that a remotely created check will be presented from time to time, and the risk management concerns are minimal. However, from the position of the bank of first deposit, the risk management concerns are heightened because of the inherent risk of unauthorized transactions. Banks' risk management programs must address their customers' use of remotely created checks to ensure the integrity of the check clearing network is preserved. Strong risk management practices such as customer due diligence at account

[93] Comments of the NCLC, supra note 3, at 5; 70 Fed. Reg. at 71,220, § 229 (the final rule's general comments state that the Board will continue to monitor developments in the EFTA and Reg. E to determine whether EFTA applies to check transactions and whether further actions is appropriate).
[94] Supra note 83, at § 21.0.
[95] Id.

origination and during the customer relationship are the first line of defense against fraudulent transactions. Because remotely created checks lack identifiers they are difficult to detect. As a result, there is no readily available quantitative data by which to measure and monitor their activity.

Estimates on the prevalence of remotely created checks vary. For example, in its comment to the Board of Governors during the proposed amendments to Regulation CC, The Clearing House stated they did not have reliable data on remotely created checks from their member banks.[96] It is difficult to quantify the total number of remotely created checks returned as unauthorized or fraudulent because check clearing control systems cannot easily detect, if at all, remotely created checks, especially since remotely created check returns are bundled with all other check returns.[97] Furthermore, banks are unable to identify and segregate remotely created checks in forward collection, making them difficult to calculate.[98] The challenge in obtaining reliable data on the number of remotely created checks in general makes the true magnitude of fraud perpetrated through this payment channel equally difficult to quantify.[99]

In an effort to better understand and measure their prevalence, the Federal Reserve Bank of Minneapolis conducted a study to estimate the number of remotely created checks based on warranty claims received by Federal Reserve Banks through the check adjustment process.[100] The Federal Reserve Bank used warranty claims as a way to measure remotely created check use because no other reliable method, other than manual examination, exists to gauge their use. Their findings revealed that a reasonably low volume of remotely created checks had entered the payments system, and that the estimated overall volumes were about the same in 2008 and 2009.

---

[96] Supra note 12; see also Crystal D. Carroll, Retail Payments Risk Forum at the Federal Reserve Bank of Atlanta, *Remotely created checks: distinguishing the good from the bad*, available at: http://portalsandrails.frbatlanta.org/remotely-created-checks/.

[97] Thomas, supra note 2, at 39.

[98] The Board proposed assigning an additional identifier to the check's MICR line. However, the Board received little support as opponents cited the proposition as impracticable, cumbersome and costly. 70 Feg. Reg. at 71,223.

[99] c.f., supra note 12 at 5, (stating that most Clearinghouse member banks have anecdotal evidence that the number of remotely created checks they process has been increasing over the years, while a few banks have anecdotal evidence that the number of incoming remotely created checks is decreasing), with Letter from National Association of Attorneys General supra note 9, at 4 (stating that one Wisconsin community bank found seventy-three percent of the remotely created checks it collected over a sixteen-month period to be fraudulent); and Thomas supra note 2, at 38.

[100] For example, according to the study, Federal Reserve Banks processed almost 2200 valid unauthorized remotely created check warranty claims in June 2009. Amanda Dorphy, Federal Reserve Bank of Minneapolis, *Remotely Created Checks*, January 2010, slide #5 (on file with author) (note that the information used in this study is based on institutions supervised by the Federal Reserve System).

Furthermore, volumes for unauthorized returns in other channels such as ACH TEL were higher at 0.13 percent compared with unauthorized remotely created checks returns at 0.03 percent.[101] This suggests that the aggregate risk exposure for remotely created checks is lower or better managed than believed, or possibly that remotely created checks' unique risk exposure due to their lack of identification does not in itself manifest unauthorized remotely created checks.[102]

Due Diligence Protocols

The increased risks associated with remotely created checks are oftentimes introduced by the poor internal controls and due diligence practices of banks in their Know Your Customer[103] programs. In the case of the third party processor, there may be an absence of any procedures required by the bank for Know Your Customers' Customer. For instance, in the InterBill case, the FTC found various instances where InterBill knew or should have known that Pharmacycards.com was running a bogus operation.[104] According to the FTC, InterBill failed to follow its own guidelines for new merchants before agreeing to do business with them, including checking references and verifying a physical address.[105]

One red flag InterBill ignored was Pharmacycards.com's proposed business model, where consumers would be mailed a negative option postcard, and if they did not respond, the consumers' accounts would be debited.[106] InterBill did not question Pharmacycards.com's business model or legal authority for withdrawing consumers' accounts without their knowledge or consent.[107] But, it was the high rates of returns, at times up to 70 percent, that the FTC alleged should have placed InterBill on notice that Pharmacycards.com's activities may have

[101] Id. at slide #6. Note that the study only looked at unauthorized returns and did not study the reason for the returns, e.g., whether returned for insufficient funds; stop payment order; closed account, but properly authorized; or returned for improper authorization.
[102] Id. at slide #3. See also Letter from Ben S. Bernanke to The Honorable Barney Frank in response to letter concerning abusive telemarketing practices, July 20, 2007 [hereinafter Letter from Bernanke] (identical letter also sent to Congressman Edward J. Markey) (in file with author) (that one year after Reg. CC's amendments to address remotely created checks took effect, board staff reviewed complaints from consumers regarding remotely created checks and did not identify any associated with remotely created checks and that banks received few requests for adjustments from paying banks for unauthorized remotely created checks).
[103] Requires banks to determine the identity of each customer, develop a profile of its customers typical account transactions and origin of the funds used, while monitoring for deviations from the established profile.
[104] Supra note 38.
[105] Id.
[106] Plaintiffs Motion for Summary Judgment and Memorandum of Points and Authorities in Support, at 5, available at: http://www.ftc.gov/os/caselist/0423192/090618interbillsjm.pdf.
[107] Id.

been fraudulent.[108] The court concluded that InterBill failed to monitor each of its client's (such as Pharmacycards.com) transactions pursuant to the TSR to ensure that none were engaged in deceptive, unfair, or abusive practices.[109] The FTC was subsequently authorized to monitor InterBill's compliance with the court's order.[110]

In efforts to further enhance due diligence protocols of national banks the OCC issued updated guidance following the conclusion of the Wachovia case, to enhance underwriting and monitoring of entities that process payments for telemarketers and other merchants, titled: *OCC Bulletin 2008-12 Risk Management Guidance*[111]. Bulletin 2008-12 was released to serve as supplemental guidance to existing risk management practices for the processing of payments for telemarketers and other merchants which pose a unique risk not present in relationships with other commercial consumers and require additional due diligence and close monitoring.[112] The bulletin outlines ways a processor uses a bank account relationship to process remotely created checks, and acknowledges that while adequate due diligence procedures exist for the banks customers, a majority of originating banks working with third party payment processors may not know or understand the nature of the transactions being submitted.[113]

Managing Remotely Created Check Fraud

Anecdotal information about remotely created check fraud is plentiful, but empirical data is sparse. An abrupt prohibition might be more disruptive than is necessary if adequate tools currently exist to mitigate the risks that remotely created checks present. Rather than outlawing remotely created checks, the banking industry and its regulators might explore the possibility that the risks associated with remotely created checks can be managed successfully without creating new costs and in ways that exceed the value of the speed and convenience of using remotely created checks for certain kinds of payment transactions.[114]

---

[108] Id. at 6.
[109] Supra note 38 at 5.
[110] Id. at 10.
[111] OCC Bulletin 2008-12, Risk Management Guidance, April 24, 2008, available at: http://www.occ.treas.gov/ftp/bulletin/2008-12.html.
[112] Id.
[113] Id.
[114] This discussion is not meant to be exhaustive, but rather highlight some of the tools that financial institutions have at their disposal for addressing the risk management of remotely created checks. For example, the FFIEC (Federal Financial Institutions Examination Council) has a booklet on Retail Payments Systems, available at:

Amendments to Reg. CC identify the depository bank as the entity in the best position to detect and prevent risky practices and fraudulent transactions. The Board, in its final rule, stated that it shifted the risk allocation of remotely created checks to the bank of first deposit because the depository bank is generally "the bank for the person that initially created and deposited the remotely created check."[115] Shifting the risk allocation from the payor to the depository bank encourages the depository bank to better manage the risk associated with remotely created checks and become more engaged with its customers' transactions involving remotely created checks.[116]

Only the bank of first deposit possesses the information that is necessary to manage remotely created check risk. At the highest level of generality, the depositary bank has the business relationship with the depositor that is creating the remotely created checks, and has a responsibility to know that customer and its business. With respect more specifically to remotely created checks, only the bank of first deposit is in a position to know the volume of items and dollars that are being deposited as remotely created checks at the bank of first deposit, and only the bank of first deposit is in a position to see the actual rate at which the remotely created checks that are deposited by its customer are being returned or are giving rise to warranty claims under Reg. CC.

In the first instance, therefore, no entity other than the bank of first deposit is in a good position to identify and manage the risks associated with remotely created checks. However, there is a significant educational and enforcement role that needs to be played by the FFIEC agencies. The agencies have the authority and responsibility to examine financial institutions for safety and soundness and for compliance with applicable laws and regulations. Clearly, there is room for the examining agencies, as part of the examination process, to educate depository institutions about the risks of remotely created checks and the need for the bank of first deposit to develop and implement risk appropriate policies and procedures to identify and mitigate risk if the bank decides to accept remotely created checks as deposits.

---

http://www.ffiec.gov/ffiecinfobase/html_pages/retail_book_frame.htm. Also, extensive guidance exists on managing third-party risk, for example, the FDIC (Federal Deposit Insurance Company), suggests there are four basic elements of an effective third-party risk management program: risk assessment; due diligence in selecting a third party; contract structuring and review; and oversight. FDIC Financial Institutional Letter FIL-44-2008, *Third-Party Risk Guidance for Managing Third-Party Risk*, June 6, 2008 (in file with author).

[115] 70 Fed. Reg. at 71,218.

[116] The Comments of the NCLC, supra note 3, at 4; Letter from The Clearing House, supra note 12, at 2.

Legal and regulatory intervention may be avoidable if the stakeholder best poised to prevent their misuse implements a comprehensive risk management program. To best position its risk management practices, the depository bank should first assess its exposure to remotely created checks by creating procedures that enable their identification through return activity and transaction monitoring.[117] A depository banks' account relationship agreement with its customers is a document that should receive close attention from a bank that handles payment transactions for its customers, whether its customers introduce remotely created checks into the check collection system or not. The account agreement could detail the number of remotely created checks it will accept for deposit within a specified period; the quality of the duplicate check image it will accept; the percentage of returns it will deem acceptable before taking further action; the ability to access from the depositor evidence of proper authorization by the drawer; or whether remotely created checks will be accepted at all.[118]

On an ongoing basis, the depository bank should perform due diligence on its remotely created check depositor to fully understand the nature of the depositor's business model and closely monitor for high return rates.[119] Upon discovering the depositor has engaged in any of the prohibited acts or violated any of the conditions established by the bank in the account relationship agreement, the depository bank should act promptly to determine whether its customer is engaging in a fraudulent act and proceed to remedy the situation.[120] For example, an exception rate that significantly exceeds the industry's normal rates of return or rejection or warranty claims with respect to a payment channel ought to operate as a red flag that triggers prompt and decisive action by a bank of first deposit. Failure to act in response to red flags, as the OCC alleged in the Wachovia case, places the depository bank in the path of potential enforcement action by regulators and law enforcement for complacent behavior.[121] It is important to not only establish prudent risk management policies and procedure, but also to

[117] See, e.g., Thomas, supra note 2, at 39.
[118] Supra note 28; see also generally, The Comments from the NCLC, supra note 3, at 4.
[119] Letter from Bernanke, supra note102, at 6; FFIEC Retail Payments Booklet 2010, supra note 115, at A-32. For example, the FFIEC (Federal Financial Institutions Examination Council) has set forth Guidance on Risk Management of Remote Deposit Capture to address the essential components of identifying, assessing, and mitigating risk, including the measuring and monitoring of residual risk exposure. Available at: http://www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf.
[120] Letter from Bernanke, supra note 102, at 7.
[121] See, e.g., supra note 46.

ensure that these practices are properly executed so that all significant risks are consistently and effectively identified, measured, monitored and controlled.[122]

If one were to assume that not every bank of first deposit is ready to do all that they should be doing to identify and manage the risks of remotely created checks, but one nevertheless believes that remotely created checks create certain efficiencies that are not created by alternative payments mechanisms, then the question becomes who can and should change the behavior of the banks of first deposit? It seems clear that the examining agencies have both an educational and a potential enforcement role to play. The examining agencies should include a review of every bank's return and exception rates for payments as part of the examination process. Where a return or exception rate is significantly above the industry norm for a payment type, the examiners should cite the financial institution for potentially unsafe and unsound practices or for risking the kind of noncompliance that resulted in the Wachovia enforcement action.

If a financial institution fails to perform its payments business with something approaching an appropriate level of due diligence, its primary federal regulator has the authority to initiate an enforcement action requiring the institution to cease and desist. If the institution has failed to police its own payments activity, and if the institution's customer has perpetrated a fraud using the bank's payments services and that fraud has resulted in harm to third parties, the lesson of the Wachovia action is that the agencies can require the financial institution to make the harmed third parties whole. Ultimately, if a financial institution knowingly processes fraudulent transactions that affect interstate commerce, the institution might be subject to civil or criminal charges.

VI. Conclusion

Depository banks, which are most closely aligned with their customers, are best poised to manage the unique risks remotely created checks present. The depository bank should have in place clear procedures outlining the appropriate due diligence and heighten account monitoring for all their customers with an underlying business activity which uses remotely created checks to serve its business needs.

[122] FFIEC, supra note 118.

Special care should be given to the risks associated with third party processors as such risk quickly rises when neither the payment processor nor the depository bank performs adequate due diligence on the merchants for which payments are originated. As evidenced in the examples provided, depository banks that do not adequately manage their customer relationships should expect to see increased regulatory scrutiny on their activities in the presentment and origination of remotely created checks.

Lastly, the bank of first deposit should recognize that initiating remotely created checks instead of ACH conversion for ACH eligible items will bypass ACH network reporting and control mechanisms that are established to help originating depository financial institutions recognize potential fraudulent situations. Therefore, and in the face of this reality, it is increasingly important that banks understand how to navigate through the new rules and risk management issues remotely created checks present, while pursuing opportunities to better identify, measure, monitor, and control their uses.

Acknowledgements:

Thanks to the following individuals for lending their expertise and insight to the development of this paper: Richard Fraher, Saidee Jackson, Albert Nazareth, Richard Oliver, Cynthia Merritt, and Julia Schein of the Federal Reserve Bank of Atlanta, Jeffrey Yeganeh of the Federal Reserve System Board of Governors, Claudia Swendseid and Amanda Dorphy of the Federal Reserve Bank of Minneapolis, Tracy Thorleifson and Allison Brown of the Federal Trade Commission, and Christopher Gill of Global Concepts Payment Systems Consulting, Devon Marsh of Wells Fargo Bank, N.A., Jane Yao of the American Bankers Association, and anyone else who entertained our many questions on this subject matter.