LOYOLA CONSUMER LAW REVIEW

Write-On Information Packet
Volume 28
2015-2016 Academic Year
LOY. CONSUMER L. REV.

WRITE-ON INFORMATION PACKET

2015-2016 Academic Year

The Loyola Consumer Law Review ("CLR") seeks to fill between 20-30 Staff Editor positions for the 2015-2016 academic year. This memorandum sets forth the write-on procedure for membership on the CLR. It also describes the responsibilities of Staff Editors and the amount of academic credit awarded.

You will have from 5:00 pm on Monday, April 27, 2015, until 11:59 pm on Friday, May 29, 2015, to complete the application. All write-on submissions must be sent to Jack Pera, News Editor, at jpera2@luc.edu. You will be notified regarding your membership status no later than July 10, 2015, unless grades are delayed beyond that date. You will have until Friday, July 17, 2015, to accept or decline your offer.

Membership is for the 2015-2016 academic year. Staff Editors receive 1 credit hour per semester for membership. This is an ungraded credit, awarded as credit/no credit.

If you have any questions, please feel free to contact Robert Gottfried, Editor-in-Chief, at rgottfried@luc.edu, or Daniel North, Executive Editor, at dnorth@luc.edu. Current CLR members, however, will not be able to give any substantive assistance on the writing competition.

Good luck!

Questions: rgottfried@luc.edu or dnorth@luc.edu
Write-On Submissions: jpera2@luc.edu
Deadline: 11:59 pm on Friday, May 29, 2015
Decisions Announced: Friday, July 10, 2015
Accept/Decline By: Friday, July 17, 2015
AN INTRODUCTION TO CLR

The Loyola Consumer Law Review ("CLR"), published three to four times per year, is the only law review of its kind in the country. The CLR is dedicated to examining legal issues as they relate to consumers. Our publication provides a forum for dialogue among practitioners, law professors, and the rest of our broad subscriber base. Because of the diversity of CLR’s subscribers, the editors strive to avoid "legalese" and heavy footnoting while maintaining the highest level of scholarship in the field.

The CLR is devoted to featuring articles regarding the effect of developing legal issues on both consumers themselves and on the practice of law as it relates to consumers. For example, recent issues have included articles on advertising, financing, debt collection, product safety, professional services, insurance, consumer credit, corporate corruption, and consumer privacy. CLR articles may be found in their entirety on Westlaw and Lexis. Many law libraries, law firms, and other organizations also subscribe to the CLR.

VOLUME 28 EDITORIAL BOARD

Editor-in-Chief
Robert Gottfried

Executive Editor
Daniel North

Managing Editor
Chuck Haskins

Publications Editor
Anna Egofske

Feature Articles Editors
Ryan Bennett
Katy Kawauchi
Cote Klinefelter

News Editor
Jack Pera

Senior Editors
Lauren Bever
Katelyn Blanchard
Ben Bresnick
Grace Chua
Dominic LoVerde
Adrienne Yoseph

Symposium Editor
Thomas Terranova
LOY. CONSUMER L. REV.

STAFF EDITOR RESPONSIBILITIES

I. Staff Edits

Staff Editors are primarily responsible for editing about two articles per semester. Each article must be thoroughly edited with great attention paid to organization, grammar, clarity, and style. Additionally, all citations must be in correct form and substance, in accordance with The Bluebook: A Uniform System of Citation. The Staff Editors will perform the initial edits on the articles. Then, Staff Editors work as needed with Senior Editors and Executive Board members to produce the final draft of each article.

Every Staff Editor must keep in contact with the Senior Editors and Board members, and must keep them informed about the status of each assignment. Staff Editors receive the benefit of putting a law school publication on their resume, as well as developing and honing their writing, grammar, legal analysis, and citation skills. Staff Editors will also have the opportunity to network and develop professional communication skills at events and conferences.

II. Orientation

As with all of Loyola’s journals, CLR members must attend a mandatory one-day orientation prior to the fall semester. Members of CLR’s Executive Board will preside over the orientation. Topics discussed will include the editing and publication process, the student article process, citations, and other topics deemed necessary by the board.

III. Student Article

To receive academic credit, each Staff Editor must produce his or her own student article of publishable quality. To accomplish this, Staff Editors must be responsible, motivated, possess excellent communication skills, and pay great attention to detail.

Student articles are analyses of recent cases, statutes, or developments in the law that have an impact on consumers. Within certain guidelines, the topic may be of the Staff Editor’s choosing. Each year, the CLR publishes a number of these student articles. Publication is a great honor, and an excellent addition to your resume.

A schedule will be provided by the Editorial Board assigning each Staff Editor a particular issue of Volume 28 for which to complete their student article.

IV. Returning the Following Year

Once a Staff Editor produces an article of publishable quality and satisfactorily completes the other duties of Staff Editor, he or she is eligible for Senior Editor position or an Executive Board position on CLR for the following year. Details about this process are released in the spring.
LOY. CONSUMER L. REV.

APPLICATION

I. Qualifications

To qualify for the CLR write-on competition, you must complete your current year in school and have the intent to return for the following full year. All J.D. students who are returning for the full 2015-2016 academic year, i.e. not graduating in December 2015, may apply. You must be a student in good standing, with a minimum GPA of 2.75. Exceptions are made only in extraordinary circumstances.

Additionally, each summer, the CLR offers Staff Editor positions to the top 15% of the incoming second-year full-time class, regardless of whether they participate in the write-on competition. These students will be contacted following the release of grades.

II. Write-On Competition – Procedures

A. Overview

The write-on competition requires applicants to write a brief article on a topic of concern to consumers. You will have from 5:00 pm on Monday, April 27, 2015 until 11:59 pm on Friday, May 29, 2015, to complete the article. You must email a Word document of your Article to jpera2@luc.edu by 11:59 pm on Friday, May 29, 2015. No late submissions will be accepted.

Identify your Student Article by placing your Student ID Number (NOT your Exam ID) on the title page and in the header of subsequent pages. Your name should not appear anywhere on your write-on submission.

Please keep a copy of your completed article, along with your notes and outlines, for ninety (90) days after you submit your application. The CLR reserves the right to examine such materials before making a decision on your application.

B. Materials to be Used

When preparing your article, you should confine your research to the sources provided in this packet. You may not read or refer to any other material on the subject of this competition, except those listed in this packet. Besides the sources attached, the only additional materials that you may consult are THE BLUEBOOK, a dictionary, and a writing guide, such as THE CHICAGO MANUAL OF STYLE. Also, to familiarize yourself with the CLR’s style, you may refer to previous CLR issues containing student articles. These are available on the bookshelves in the CLR office, Room 1434, or online at www.luc.edu/law/student/publications/clr. You may not, however, use these additional materials in a substantive way. By limiting the materials you may use, the CLR hopes to encourage analysis over research.
You need not use every source listed in the packet. Determine which sources are most relevant to the arguments you wish to make.

C. Citations

All citations used in your article need to be in the form of footnotes and must conform to The Bluebook citation guidelines. Correct citation format will be a substantial factor considered in your application.

D. Footnotes

Footnotes are for citation and discussion of tangential issues, or for the inclusion of supplemental materials. Only major cases should be named in the text of the article. No citations should appear in the text of the article – only in the footnotes. Consult The Bluebook for the form of citations in law review articles. All citations must conform to The Bluebook: A Uniform System of Citation.

All quotations or ideas taken from any source must be cited in the footnotes. You may also indicate in your footnote citation if your source is itself relying on another source. Again, consult The Bluebook for the form of these citations. Only matters that are entirely your own ideas and your own writing maybe left without citation.

E. Form of the Writing

Articles must be typed on 8-1/2” x 11” plain white paper. The text must be double-spaced with one-inch margins on all four sides using 12-point Times New Roman font. Footnotes must be single-spaced. The article must be between 4-8 pages in length, excluding the title page. No material beyond 8 pages will be considered. Each page after the first must be numbered at the bottom-center of each page.

F. Writing Style

Good writing style is extremely important. Pay particular attention to grammar, word choice, sentence and paragraph structure, and transitions between paragraphs and sections. Make sure your writing is clear and interesting. You may look to recent copies of the CLR to see examples of appropriate CLR style. Copies are available in the CLR office, room 1434, or online at www.luc.edu/law/student/publications/clr.

Clear writing requires clear analysis. Given the limited length of your article, give particular thought to how much space you devote to certain issues, and what may more appropriately belong in a footnote rather than in the text.

G. Evaluation

Your article will be evaluated based on several factors, including: accurate legal analysis, proper citation form, good use of footnotes, clear and concise writing style, correct grammar, and
coherent organization. Additionally, your grade point average may be weighed in as part of the evaluation process.

F. Confidentiality and Plagiarism

You must work entirely on your own; the write-on is an individual effort. You may not receive any substantive, editorial, or proofreading assistance, nor may you discuss any aspect of the article with any other person before all applications are submitted.

Plagiarism includes, but is not limited to, failing to attribute language or ideas to their original source, or failing to indicate a quotation of five or more consecutive words. Plagiarism is strictly forbidden and offenders may be subject to discipline by Loyola University Chicago School of Law.

III. Write-On Competition: Subject and Format

A. Explanation of the Problem

This year’s write-on competition will focus on emerging payments and relevant consumer protection concerns. You should read the materials provided for the topic given and analyze the impact of the selected topic on consumers. You should organize your discussion using a traditional “note” format. See a recent copy of the CLR for an example of a student article.

Since the CLR wishes to emphasize analysis over research when selecting its members, this competition is a closed research assignment. You are to consult only those sources included in this write-on packet. Any deviation from this rule will result in disqualification from the competition. However, you need not reference all of the sources listed below in your article. Only cite to what you think is appropriate, however, consideration will be given to creative and efficient use of most of the sources.

B. Format of the CLR Student Article

The CLR write-on is designed as a note analyzing a current issue impacting consumers. In addition to informing the reader of the various aspects of the issue in question, the CLR note should take a position on the effect of the selected topic on consumers. The best submissions will persuasively use the available sources to support the position taken. A typical CLR note includes the following sections, although you may use different names for headings and subsections as you see fit:

I. Introduction

This is one of the most important parts of the article. It sets the stage for everything that follows. The introduction should define the issue to be discussed and tell the reader why the issue is important. The introduction should also provide the reader with a roadmap describing the topics you will cover, and the basic outline of the article, including the argument you are going to make. Be sure to follow through with any promises you make in the introduction.
II. Background

This will be brief for purposes of the write-on. The background section should provide more than just a historical report. It should involve some analysis, such as explaining the issue of law involved, identifying any underlying trends or significant events, and highlighting the areas that you will be returning to later as you analyze the topic. The background section should set up and lead naturally to a discussion of the issue.

III. Analysis/Impact

In this section, unleash your creative tendencies and argue for your point of view on the issue. Give your own critical analysis of the effect of these laws, regulations, etc. on consumers, and support your arguments with facts and ideas developed in your background section.

IV. Conclusion

Give a brief summary of your conclusions. This section generally should not be more than a paragraph or two.

IV. REMEMBER

- Submissions should be within 4-8 pages, 1-inch margins, 12-point Times New Roman font, including footnotes, but excluding the title page. Footnotes must be single-spaced. Text must be double-spaced. Not all source material need be cited. Number each page at the bottom-center, omitting a page number on the first page.
- All citations must conform to The Bluebook.
- Put your Student ID Number on the title page and in the header for each subsequent page. Do not put your name anywhere on your submission.
- Submissions are due to Jack Pera, News Editor, at jpera2@luc.edu, by 11:59 pm, Friday, May 29, 2015.
- Any questions may be directed to Robert Gottfried, Editor-in-Chief, at rgottfried@luc.edu, or Daniel North, Executive Editor, at dnorth@luc.edu.

GOOD LUCK!
SOURCES
LOY. CONSUMER L. REV.

WRITE-ON SOURCE LIST


3. Letter from Americans for Financial Reform

4. National Consumer Law Center: Protections Needed for Prepaid Payroll, Unemployment Benefits, Child Support, and Other Prepaid Payment Cards

5. Electronic Payments in the U.S. Economy: An Overview, Stuart E. Weiner, Federal Reserve Bank of Kansas City

6. IMF Report: Role and Security of Payment Systems in an Electronic Age; Mark Fajfar

7. In re Visa Check/MasterMoney Antitrust Litigation


10. Venmo Money, Venmo Problems; Alison Griswold; http://www.slate.com/articles/technology/safety_net/2015/02/venmo_security_it_s_not_as_strong_as_the_company_wants_you_to_think.single.html
The Changing Face of the Payments System:
A Policymaker’s Guide to Important Issues
About the ABA and this Paper

Founded in 1875, the American Bankers Association (ABA) represents banks of all sizes and charters and is the voice for the nation’s $14 trillion banking industry and its two million employees.

Earlier this year, the ABA formed a consortium of banks to study the evolving retail payments market. This group, the Emerging Payments Advisory Group (EPAG), has 13 bank participants spanning all bank sizes and geographies.

The ABA, in consultation with this group, identified a number of critical issues facing the retail payments market. This paper is the result of these discussions and is intended to assist in the ongoing policy dialogue. Its focus is on the importance that innovation, consumer protection, competitiveness and safety and soundness play in the ongoing debate over the changing face of the US payment system. It is not intended to provide answers to all the questions that will inevitably arise, but to call attention to critical issues for policymakers to consider as they debate the future of payments system regulation.

For the sake for brevity, this paper only discusses a subset of the key issues involved with payments and, for these, identifies some—but not all—of the most salient considerations. For a more complete discussion of the issues and key considerations, the reader is encouraged to contact the ABA directly.

The ABA wishes to thank Tony Hayes and Andy Dresner of Oliver Wyman for their invaluable assistance in facilitating EPAG discussions, helping the group identify industry priorities that became the basis of this report. That said, the views expressed in this report are solely those of the ABA.
The Evolving Payments Market

Background

The U.S. payments market continues to shift away from cash and paper checks toward various forms of electronic payments. Credit cards and debit cards are now commonplace, and general purpose reloadable prepaid cards are expanding the overall customer base. For instance, the U.S. Treasury now recommends a prepaid card as a payment option for federal benefit recipients who lack a bank or credit union account, and over two million consumers now utilize this option on a recurring basis.

Beyond cards, the payments market is more dynamic than ever. In some stores, consumers can now pay by simply tapping their phones on the retailer’s payment terminal or by showing a barcode on their smart phone’s screen. Similarly, as e-commerce expands, so do the number of ways to pay online.

Innovation

Our once cash-based society has evolved through checks, into cards, and is now pushing into a digital frontier of virtual “wallets” and mobile platforms. Innovators span the gamut from traditional players doing new things to new players performing similarly traditional functions (e.g., PayPal, Square), while at the extreme end, others are attempting to bypass the existing payments system entirely (e.g., Bitcoin). The common thread is that all of them are continually seeking new ways to assist consumers and businesses in the way they make purchases. Banks—which developed the first credit card in 1958 and have since pioneered technologies like online banking and billpay, mobile banking, and remote check deposit capabilities—continue to push the innovation envelope to improve the banking experience for consumers and businesses. Additionally, several large nonbanks are now active in the payments sector, including PayPal, Walmart, Google, Square, and telecommunications operators such as AT&T, Verizon and T-Mobile. With so much activity, the most successful will be companies that deliver superior benefits to the overall payments ecosystem.

EXHIBIT 1

A virtual, or digital, “wallet” is generally an electronic medium that allows consumers to facilitate transactions, and are often linked with one or more bank accounts or payment cards.
Implications

With marketplace innovation in both payment methods and participants comes important policy issues for Congress and federal regulators to consider. On the one hand, it is important to encourage marketplace innovations that promote consumer convenience, transaction efficiency, competition and overall benefits to the U.S. economy, free of overly inhibiting government regulation. On the other hand, it is also important that adequate protections be built into any regulatory framework so that consumer confidence in the U.S. payments system remains at the level we all currently experience and have come to expect.

Achieving the right balance in this policy debate is important, as it has enormous implications for the U.S. economic system. Accordingly, this paper attempts to identify three key areas in the emerging and mobile payments landscape that we believe deserve policymaker attention:

1. Consumer Protection: Federal law provides numerous protections for consumers when they make electronic payments, such as protection against unauthorized charges and defined procedures for disputing any charge. With this foundation in place, consumers have come to expect equal protection across all electronic payment types, regardless of the particular product or provider or its status as a bank or nonbank. However, in many cases today (particularly with respect to nonbank participants), regulations for emerging payments are either uneven or not well-defined, with a potential to result in consumer harm, material breaches of privacy and degradation to the current consumer protection scheme.

2. Payment System Integrity: Payments facilitate all forms of commerce, and as a result, the overall stability, efficiency and integrity of the payments system are of paramount importance. In short, the system must “always work.” All participating institutions—whether they are banks, payment networks, telecommunications companies, high tech firms and the like—must maintain necessary controls and be subject to sufficient government oversight to ensure that the integrity of the payments system is never in question. Moreover, payments system providers have become important government partners in enforcing various federal laws meant to combat illegal money laundering, threats to our nation’s cybersecurity, and other important policy initiatives. The degree to which new participants in the payments space maintain adequate controls that facilitate overall payments system integrity remains a critical policy question to explore.

3. Competitive Equity: Banks, retailers, networks and others have all made significant investments in the U.S. payments infrastructure. As these systems have grown and incorporated new technologies, the rules and standards governing them must evolve to accommodate these advances. A common sense of fairness argues that all participants, whether incumbents or new entrants, operate by a similar set of rules and standards. This ensures that all participants have parallel financial incentives to innovate, and eliminates anomalies in the market driven solely by government policies that apply to some players but not others.

What follows is a brief overview of how the payments market is changing, along with a more in-depth look at each of the key areas outlined above.
1. Consumer Protection

Key Questions:

- Does the payment method provide consumer protection consistent with federal regulation?
- Are consumers’ rights clearly disclosed and easily understood?

Advances in technology and communications are allowing new providers—tech companies, communications firms and the like—to create new payment methods that are not contemplated by the current regulatory framework. In short, such advances potentially leapfrog existing statutory consumer protections, depending on how the transaction is structured.

The flow-chart below reflects the changing infrastructure behind some of the emerging payments coming to market today. While the existing systems to process debit and credit card transactions are complex, they do not contain as many actors, nor do they involve as elaborate a chain of communication. As a technical matter, regardless of what technology a consumer utilizes in a transaction, the technology itself must have a way to access the consumer’s funds. From a consumers’ perspective, all that is important is that the transaction is processed seamlessly, safely and efficiently, and with the legal protections regarding such things as disclosures, privacy and fraud that exist under current law. The question is, depending upon the role of new entrants in the payments space, do these legal protections apply, to whom and to what extent?

Mobile wallet transaction involving a pre-funded wallet
Existing Protections Establish Clear Consumer Rights

With a traditional card payment, the rights and obligations of all parties are well-defined by federal statute. For example, Regulation E describes consumers’ rights and card issuers’ obligations when a debit card is used, while Regulation Z does so for credit card transactions. The payment networks such as Visa and MasterCard also have well-established rules for merchants and issuers, which provide further protections. For instance, while Regulation Z limits a customer’s liability for unauthorized transactions on a lost or stolen credit card to $50, the card networks require issuers to provide their cardholders with zero liability. Not only does the consumer have clear rights, but also the parties responsible for these protections are clearly articulated.

Newer Technologies, Unclear Rules

New technologies have the potential to fundamentally reshape the existing payments infrastructure. While this is an exciting prospect, it also means that today’s rules governing the system are not likely to adequately address the payments landscape of tomorrow.

For example, a nonbank payment provider may link a smart phone service to a conventional bank service, such as ACH, debit transactions or a credit card or debit card. These may be two separate transactions. The nonbank payment service provider pays the merchant and, in a separate payment transaction, the customer’s bank pays the nonbank payment service provider. Nevertheless, these two transactions may be perceived by the consumer as a single transaction. However, the nonbank transaction may not be subject to the consumer protections of the Electronic Funds Transfer Act (EFTA). Even if the EFTA applies, or the nonbank payment service provider treats it as applying, consumers are almost certain to be confused about how to assert their rights for errors or unauthorized transactions. For example, if an unauthorized or erroneous transaction occurs, should consumers go to their bank or the nonbank service provider? Will their bank, which paid the nonbank service provider, be able to identify the merchant that was paid by the nonbank payment service provider (as sometimes this information is hidden from the bank), or have a process for resolving the dispute with that merchant?

Most consumers today have a good grasp on who to call in case of a problem or disputed transaction. Tomorrow, however, that may not be the case. Scenarios such as the one described above present questions that are not clearly answered by existing regulation. Regardless of the payment provider or payment technology, consumers should be entitled to a certain minimum threshold level of protection when making any form of payment and clarity with regard to their rights.

2. The Electronic Funds Transfer Act was enacted in 1978 in the earliest days of electronic payments. Its implementing rules, known as “Regulation E,” are intended to protect consumers from errors and fraud that could occur in electronic transactions.
2. Payment System Integrity

Key Questions:

- Does the nonbank payment provider adhere to all government and regulatory programs to maintain the safety and soundness of the payment system?

- If not, and because the provider currently falls outside the existing payments regulatory framework, does the provider introduce a potential weak link into efforts to safeguard the U.S.?

Marketplace Evolution

To borrow from the old saying: a payments infrastructure is only as secure as its weakest link. As online payments and mobile payments become more popular, consumers are increasingly storing their payment credentials on multiple websites. And as the vulnerabilities of payment card magnetic stripes continue to be exploited in larger numbers, issuers are looking to technology to improve their fraud protection capabilities.

Here are some examples of developments in the marketplace:

- To pay online, consumers create an account with the e-commerce provider and register their payment card(s). Now, when it’s time to pay, consumers can simply check out rather than having to enter their card information, billing address, shipping address, and other relevant details. In this way, Amazon, Apple’s iTunes and other online retailers reduce “friction” in the consumer shopping experience.

- Brick-and-mortar retailers are also encouraging customers to register their payment cards, either to receive discounts or to link them to the merchants’ loyalty programs.

- Increasingly, mobile wallet providers require consumers to store their account details on their smart phone (or make them accessible to the phone), so that the phone can be used to initiate payments.

- Payment card networks, card issuers and merchants in the U.S., seeking to keep pace with evolving technologies and increasingly savvy criminals, are—among other things—in the process of implementing a chip technology known as EMV (see the sidebar on the next page).

There’s no question that these services offer convenience for consumers. But there are also important policy questions that need to be addressed.

3. Usually a credit or debit card number, or account information linking to a consumer’s checking account.
System Security

First, is every database that houses payment account credentials secure? Who is responsible for overseeing and regulating the safety and soundness of these providers?

Historically, since banks hold the funds and bear the risk, banks were the only parties with access to payment credentials. When a payment card is used, the information is encrypted and sent from the merchant to the network to the issuer to be decrypted and processed. The Federal Reserve and other bank regulators, plus each bank’s prudential regulator, regularly audit banks to verify the security of these payment credentials and the underlying accounts.

Moreover, through control over the payment system, the government and regulators help enforce existing laws. Examples include: bank Know Your Customer (KYC) requirements and Anti-Money Laundering (AML) laws; requirements to file Suspicious Activity Reports (SARs); a prohibition on certain foreign nationals (SDNs) from accessing the U.S. financial system; the obligation of banks to check their customers against a list of known problem countries and/or companies (e.g., the OFAC database); and, a prohibition on the use of payment cards for online gambling.

Now, with numerous nonbanks involved with payments and storing payment account information, is there a regulator (or regulators) tasked with ensuring that they are also maintaining adequate safeguards or otherwise assisting in those government mandates?

While many large nonbank organizations are likely to follow leading industry practices for securing payment information, there is no guarantee that that will be the case, to what extent they are prepared for unanticipated events (e.g., cyber attack), or how such compliance would be assured through regulatory enforcement. Moreover, it is unclear if the same level of care will be practiced by smaller technology startups. It is possible that some companies will focus on delivering a great user experience and give less attention to the “plumbing” of securing payment card information. Yet, if this database is ever compromised, the biggest loser might not be the company with inadequate security, but its users and all of the banks that issued cards to these consumers.
**Identifying the Merchant**

Another important issue with respect to mobile payments concerns a particular approach to transaction routing.

With most payments, the consumer initiates a payment at a store by using a card and the bank approves the transaction. The consumer’s bank statement subsequently lists the purchase date, amount, and store name.

With some forms of mobile payments, however and as noted previously, the purchase is actually split into two steps: first, consumers initiate a payment at the merchant with their phone; second, the mobile payment provider withdraws the appropriate amount from the consumer’s linked bank account or payment card. To the bank, this transaction no longer looks like a purchase by their customer from a particular merchant but instead appears as a transfer request to an intermediary payment provider.

Here’s why: with some mobile providers configured as the Merchant of Record (MoR), the wallet provider appears as the “merchant,” rather than the actual merchant. As a result, the consumer statement no longer provides the actual name but the intermediary’s information. Additionally, if the intermediary aggregates transactions, such that several purchases translate into one debit against the consumer’s account, it is recorded as such and becomes problematic to dispute and reverse a specific item.

For example, what used to appear on a consumer’s account statement as a $150 purchase from “ABC Hardware Store”—a description likely to jog a person’s memory of the transaction—could now appear as a $150 transaction from “Wallet Provider X.” If the wallet provider chooses to aggregate transactions over a period of time, then a series of transactions from any number of merchants made by a consumer could appear as a single “$1,100 Wallet Provider X” notation on a monthly statement.

Besides the obvious potential for consumer confusion, this approach can undermine banks’ fraud prevention efforts, since without accurate merchant information, it is more difficult for issuers to detect how a series of transactions looks like suspicious activity and block fraudulent purchases.

Linking transactions on a one-for-one basis, and ensuring that every transaction is mapped to the actual merchant, would greatly enhance efforts to preserve the overall integrity of the payment system.
3. Competitive Equity

Key Question:

- Is the payment provider subject to the same rules and oversight as other market participants?

Regulatory Differences

Regulated banks, by the nature of their charters, clearly meet the test of financial soundness and responsibility—a primary reason why payment system participants feel confident using the system to process tens of billions of transactions each year.

- Depository institutions have an extensive system of regulation and supervision of their controls and ability to carry out payments system services, designed specifically to protect the industry’s safety and soundness.

- They are likewise subject to a stringent consumer protection regime that ensures adequate disclosures, limits fraud liability and protects a customer’s privacy.

On the other hand:

- Nonbanks providing payments system services are not regularly examined by federal financial agencies with regard to their payments system activities.

- The oversight capabilities of the Federal Trade Commission are not adequate to the task of ensuring that adequate safeguards and consumer protections are in place. The FTC has the authority to set standards for safeguarding customer information by nonbanks under section 501(b) of the Gramm-Leach-Bliley Act. However, ensuring compliance with these safeguards remains problematic because the FTC does not have the resources to conduct prophylactic examinations of businesses that are expected to follow its regulations. The FTC is able to conduct investigations based on complaints or after breaches become public knowledge, but by then the damage has already been done—to customers, but perhaps also to the payments system more broadly.

In order to ensure that all stakeholders in the payments system—including consumers, banks and nonbanks—are protected from financial, reputational, and systemic risk, all entities providing payment services should be subject to similar standards and cost structures so as to not drive the market to poorly regulated segments. Otherwise, less-regulated entities (i.e., nonbanks) will rush to offer enticing products that skirt the edges of traditional banking regulations, yet often contain terms and conditions that are not in consumers’ best interests.

Barriers to Enhanced Competition

Differential rules have other implications, namely driving market product innovation to certain market providers and away from others, often solely based on arbitrary policy judgments.

One illustration of this is the so-called Durbin Amendment, which imposed price controls on debit card interchange revenue for only certain market participants (i.e., banks with over $10 billion in assets) and certain products (i.e., debit cards). This creates market incentives to innovate away from certain products (i.e., debit cards) and towards other products (i.e.,
prepaid cards). It likewise forces some market participants to limit the consumer utility of their products—in this case, for example, some larger banks cannot offer prepaid cards with automatic bill-paying functions without being subject to Durbin price controls, while others face no similar revenue restriction. In the end, it’s consumers that lose as they no longer have the option to choose beneficial products from the widest range of competitors. Such arbitrary line-drawing by policymakers restricts the ability of all market participants to compete on equal footing, denying consumers the benefit of that innovation and competition.

The Big Picture

These regulatory gaps are particularly important for the operation of the payments system, where uninterrupted flow of funds is expected and relied upon by customers. Nonbanks do not normally have this layer of preventative protection. The importance of the integrity of the payments system and the increasingly significant role played by nonbank firms in offering payments services suggests that this issue should be addressed by federal authorities sooner rather than later, before significant disruptions to the payments system caused by nonbank failure to perform occur. Failure to do so runs the risk of incentivizing the creation of a “shadow payments system” outside of existing consumer protection and system integrity schemes, with enormous implications for consumers and the overall economy.

Conclusion

The payments ecosystem is one of the most fertile sectors of innovation in the economy today. Banks and nonbanks, established companies and garage-based start-ups, brick-and-mortar retailers and online pioneers—all are competing for the hearts, minds and wallets (literally and virtually) of the American consumer. Which technologies will have the widest acceptance has yet to be determined, but the path to get there will be an exciting one and likely driven by consumers’ concerns about liability, exposure to fraud, fees, privacy and reliability.

Today, the seamless—almost invisible—operation of the nation’s payments system is largely taken for granted. But the lessons of history must not be forgotten. Without proper safeguards the system can break down, particularly as criminals seeking to compromise the system increase their sophistication. As new technologies and payment instruments are introduced, it is crucial to ensure they do not present significant, unnecessary risks.

The existing framework for regulating and supervising banks provides consumers with the fundamental assurance that institutions engaged in payments activities operate in a safe and sound manner. While the current system is not a guarantee against isolated problems, it does serve to maintain the public’s trust in the integrity of the overall system, a virtue that must be preserved.

The banking industry is well-positioned to continue its vital role as a premier provider of innovative payments system services. As U.S. policymakers continue their examination of the changing face of payments and begin to consider applying a regulatory framework to these new market entrants, it is clear that many parallels could be drawn between the existing waterfront of bank regulations and new, emerging payments players. While a one-size-fits-all approach may not be appropriate, certainly concepts from the existing body of payments statutes—particularly as they relate to consumer protection and ensuring the integrity of the overall payments system—can and should be applied fairly to all participants.
Bitcoin or Mobile Payments? Consumers Say Cash Is the Most Secure Way to Pay

By Inside Bitcoins  Mar 4, 2015 9:25 AM EDT
NEW YORK (InsideBitcoins) — If consumers are to embrace bitcoin as a method of payment in their everyday life, there’s still a long way to go. Only 3% of those surveyed by marketing agency Walker Sands believe bitcoin — or any cryptocurrency — is the most secure way to issue payments. But inexplicably, one of the fastest growing payment methods is trusted even less: mobile wallets and smartphone apps.
Just 1% of those surveyed think smartphones are the most secure form of payment. The most secure way to pay? With cash, according to 56% of the respondents.

In spite of the hand-wringing over security, mobile payments are rapidly growing in favor. While only 4% of consumers said they had tried Apple Pay in the past year, 18% said the introduction of Apple Pay makes them more likely to make a purchase on their phone in the near future.

“Apple has the potential to help mobile payments go mainstream in 2015 by raising awareness and setting industry standards,” the Walker Sands report says.

But the transition to mobile payments might be more gradual than industry insiders would like.

“But Apple and other leaders in the mobile payment space will need to overcome several consumer concerns before smartphone payments compete with the convenience of credit cards,” the report adds, despite numerous high-profile hacks of credit and debit cards.

---

**Event schedule**

- **Chicago** • July 10-11, 2015
- **London** • September 2015
- **Seoul** • December 10-11 2015
- **San Diego** • December 14-16, 2015
July 15, 2014

Representative
United States House of Representatives
Washington, DC 20515

Re: Support Operation Choke Point and other efforts to fight payment fraud; oppose bills to curtail payment fraud work

Dear Representative:

Americans for Financial Reform and the undersigned community, consumer and civil rights groups urge you to support efforts to ensure that banks and payment processors avoid facilitating illegal activity by complying with longstanding due diligence requirements to know their customers, monitor return rates, and be alert for suspicious activity. Please oppose any bills to defund or weaken efforts to fight payment fraud or to insulate banks or payment processors that do not conduct appropriate due diligence or ignore red flags. We need every tool to fight data breaches, identity theft, scams, frauds, money laundering, and other illegal conduct.

**Fraudsters Need Banks and Payment Processors to Access the Payment System**

Many scams, frauds and illegal activity could not occur without access to the payment system. Banks and payment processors that originate payments play a critical role in enabling wrongdoers to debit victims’ bank accounts and to move money around. Examples of unlawful activity that would not be possible without an originating bank include the following:

- A telemarketing scam defrauded seniors of $20 million by lying to them to get their bank account information.¹
- A lead generator tricked people who applied for payday loans and used their bank account information to charge them $35 million for unwanted programs.²
- Bogus debt relief services scammed consumers out of $8 million and made their debt problems worse.³
- Wachovia Bank enabled $160 million in fraud by scammers targeting vulnerable seniors.⁴
- After an enforcement action against Wachovia, scammers moved their business to Zions Bank, which allowed it to continue despite spotting suspicious activity. For example, a
telemarketer calling a senior about a purported update to his health insurance card tricked him into revealing his bank account information.5

The FBI estimates that mass-marketing fraud schemes causes tens of billions of dollars of losses each year from millions of individuals and businesses,6 and one study found that fraud drains $2.9 billion a year from the savings of senior citizens.7 In addition, the data obtained in breaches like the recent Target, Michael’s and P.F. Chang breaches would be useless without a bank to use that data to debit bank or credit cards accounts.

Banks are not always aware that they are being used to facilitate illegal activity. But when they choose profits in the face of blatant signs of illegality, they become an appropriate target for enforcement action. Indeed, if regulators do not take action against banks or payment processors facilitating illegal payments, they are left playing an impossible game of ‘whack a mole’ which makes it much too easy for fraudsters to get away with continuing to break the law, and processing institutions to continue to benefit from law-breaking.

**Payment Fraud Hurts Everyone**

Wrongdoers who access the payment system inflict harm on everyone. In addition to the direct victims of fraud, the general public spends millions of dollars on identity protection products and loses faith in the security of the payment system. Retailers and online merchants lose business if consumers are afraid to shop on their website or at their store. Consumers’ banks bear the customer friction and the expense of dealing with unauthorized charges. The fraudsters’ banks and payment processors may suffer regulatory or enforcement actions, lost customers, private lawsuits, and adverse publicity. American security is also put at risk when banks and processors that lack know-your-customer controls are used for money laundering for drug cartels, terrorist groups, and other criminals.

**DOJ’s Operation Choke Point**

The Department of Justice’s (DOJ) Operation Choke Point is aimed at banks that “choose to process transactions even though they know the transactions are fraudulent, or willfully ignore clear evidence of fraud.”8 The focus is on illegal conduct, not activity that DOJ deems immoral.

The first, and to date only, action that DOJ has brought as a result of Operation Choke Point is U.S. v. Four Oaks Fincorp, Inc., Four Oaks Bank & Trust Co. Four Oaks enabled payments for illegal and fraudulent payday loans; an illegal Ponzi scheme that resulted in an SEC enforcement action;9 a money laundering operation for illegal internet gambling payments;10 and a recidivist prepaid card marketing scam that made unauthorized debits for a bogus credit line.11 DOJ charged that the bank ignored blatant red flags of illegality, including extremely high rates of payments returned as unauthorized; efforts to hide merchants’ identities; offshore entities clearly violating U.S. laws; disregard for Bank Secrecy Act obligations by foreign entities; hundreds of
consumer complaints of fraud; and federal and state law violations, including warnings by NACHA and state attorneys general.

This type of disregard for know-your-customer requirements and the legality of payments is what led to last month’s $8.9 billion penalty against BNP Paribas for concealing billions of dollars in transactions for clients in Sudan, Iran and Cuba,12 and to a $1.92 billion penalty against HSBC for helping terrorists, Iran, and Mexican drug cartels launder money.13 It is impossible to read the Four Oaks complaint without concluding that Operation Choke Point is essential work for which DOJ should be applauded, not criticized.14 Calls to abandon Operation Choke Point are misguided and inappropriate.

**Regulators Have Appropriately Warned Banks to be Aware of High-Risk Activities, But Banks Need Not Reject Legal Businesses**

Separate from DOJ’s Operation Choke Point, bank regulators have asked banks to be aware of higher-risk activities, defined as areas with a “higher incidence of consumer fraud or potentially illegal activities.”15 As with Operation Choke Point, the focus of bank regulators is on areas where fraud or illegal activity is prevalent. For example, telemarketing, credit repair services, and debt forgiveness programs have long been problematic areas plagued with fraud and deceptive conduct. Payday lending is a high-risk activity because it is completely unlawful in 15 states, is unlawful in nearly every other state if the lender lacks a state license, and, especially for online lending, often results in repeated debits that the consumer did not knowingly authorize.

Regulators have also made clear that banks that “properly manage these relationships and risks are neither prohibited nor discouraged” from providing services to lawful customers in high-risk areas.16 Banks need only be aware of the potential for illegal activities; know their customers, including basic due diligence of high-risk businesses;17 monitor payment return rates; and be alert for suspicious activity. These are not new obligations, but they are essential ones.

Some recent headlines have drawn sweeping, unsubstantiated conclusions based on individual bank account closures. Banks close accounts every day for a variety of reasons. The bank that closed the account of the adult entertainer, for example, has stated unequivocally that it was unrelated to either Operation Choke Point or any policy concerning her profession.18 The same is true of a gun dealer who was cut off by its payment processor.19

Even the National Rifle Association has said:

“[W]e have not substantiated that [anti-gun groups’ efforts] are part of an overarching federal conspiracy to suppress lawful commerce in firearms and ammunition, or that the federal government has an official policy of using financial regulators to drive firearm or ammunition companies out of business.”

Concerns by payday lenders that they are being rejected by some banks go back a decade or longer, long before the 2013 Operation Choke Point or the FDIC’s 2011 guidance on payment
processing relationships. For example, in 2006, the Financial Service Centers of America (FiSCA), which represents check cashers, money transmitters and payday lenders, testified:

“For the past six years [since 2000] banks have been abandoning us - first in a trickle, then continuously accelerating so that now few banks are willing to service us …”

Anecdotes about a few closed accounts do not prove regulatory overreach. The bank could have seen signs of illegality; terminated a problematic processor that had both illegal and legal clients; terminated businesses that lacked adequate controls; made its own business decision to cut ties with payday lenders after the bank suffered adverse publicity from its own payday lending; or misunderstood inflammatory headlines and regulatory signals.

Some bank account closures may also be related to anti-money laundering (AML) and Bank Secrecy Act issues that are separate from whether the business is considered a high-risk business. Some payday lenders with state licenses are also check cashers and money transmitters, areas that require compliance with complicated but important AML rules. Recent money laundering settlements may have drawn more attention to those rules, and the fact that Operation Choke Point is now in the news does not mean that every bank account closure is related.

Regulators are working to clear up any misconceptions created by overreaching headlines or exaggerated lobbyist claims, while also emphasizing the importance of work to prevent payment fraud. As FDIC Vice Chairman Thomas M. Hoenig said recently:

[I]f the bank knows its customer, takes the necessary steps, has the right controls, then they ought to be able to engage with them…. But you need to do those things like BSA [compliance]…. I do believe we have an obligation to say, “If you are following these rules, [you] have to then judge the risk that [you] are willing to take on.” That’s the process and I’m very comfortable with that.

It is irresponsible and dangerous to halt scrutiny of banks and payment processors that close their eyes when they operate in areas with a high risk of illegality. There are thousands of banks in this country and plenty that will continue to handle high risk but lawful accounts. But the tens of billions of dollars that Americans lose to fraud every year and the harms permitted by money laundering are just too great to abandon all vigilance by banks and payment processors that are in a position to stop illegal activity.

**Small Banks are Not a Target But May be Disproportionately At Risk**

Banks large and small have received subpoenas and enforcement actions related to payment fraud. But small banks may be disproportionately likely to process illegal payments or be harmed by payment fraud. Some fraudsters target small banks that lack the internal controls to spot suspicious activity or that (like Four Oaks Bank) need capital and look the other way in exchange for fee income. High risk activities without due diligence are also more dangerous to the safety and soundness of a small bank.
Moreover, more small banks are hurt by payment fraud than facilitate it. When the scammer’s bank submits an unauthorized charge against a consumer’s account, the consumer’s bank incurs expenses to deal with the mess. Those costs can be substantial for small banks. When a consumer contests an unauthorized payment, the average bank cost for handling a return is $4.99. But for a small bank the cost is much higher: the average is over $100 and can be as high as $509.90, according to NACHA, the Electronic Payments Association.22

The disproportionate impact of payment fraud on smaller banks is a reason to continue efforts to stop illegal activity. It is not a reason to halt such efforts.

**Conclusion**

Fighting payment fraud should not be controversial. Everyone benefits from efforts to stop illegal activity that relies on the payment system. We urge you to support efforts to ensure that banks and payment processors do their part and to hold them accountable when they fail to comply with know-your-customer requirements, conduct due diligence on high-risk activities, or overlook obvious signs of illegality.

Yours very truly,

Americans for Financial Reform
Arizona Community Action Association
Arkansas Against Abusive Payday Lending
California Reinvestment Coalition
Center for California Homeowner Association Law (Oakland, CA)
Center for Economic Integrity (Arizona)
Center for Responsible Lending
Coalition of Religious Communities
Chicago Consumer Coalition
Consumer Federation of America
Consumer Action
Consumers for Auto Reliability and Safety
Consumers Union
Economic Fairness Oregon
Florida Alliance for Consumer Protection
Kentucky Equal Justice Center
The Leadership Conference on Civil and Human Rights
National Association of Consumer Advocates
National Consumer Law Center (on behalf of its low income clients)
National Fair Housing Alliance
National People’s Action
New Economy Project
NW Consumer Law Center
Public Citizen
Public Justice Center
Reinvestment Partners
South Carolina Appleseed Legal Justice Center
Texas Appleseed
U.S. PIRG
Virginia Citizens Consumer Council
Virginia Partnership to Encourage Responsible Lending
Virginia Poverty Law Center
Woodstock Institute


17 For example, it is a simple matter to ask a payday lender in what state it lends and to show that it has licenses in those states.

18 Dana Liebelson, “Is Obama Really Forcing Banks to Close Porn Stars’ Accounts? No, Says Chase Insider,” Huffington Post (May 8, 2014), available at http://www.motherjones.com/politics/2014/05/operation-chokepoint-banks-porn-stars (quoting Chase source as saying: “This has nothing to do with Operation Choke Point … we have no policy that would prohibit a consumer from having a checking account because of an affiliation with this industry. We routinely exit consumers for a variety of reasons. For privacy reasons we can’t get into why.”).

19 Red Wing Ammunition Co. “isn’t sure why he was cut off” by First Data, which stated: “First Data processes transactions for merchants selling firearms and ammunition, so long as they meet our longstanding credit/risk management policy requirements… These policies were implemented before the DOJ’s Operation Choke Point and are unrelated.” Jennifer Bjorhus, Star Tribune, “Federal antifraud initiative goes too far, banks say” (June 7, 2014), available at http://www.startribune.com/business/262167821.html.

21 Kate Davidson and Zachary Warmbrodt, Q&A: Thomas Hoenig, Politico Pro (June 13, 2014).

22 NACHA-The Electronic Payments Association, “Improving ACH Network Quality by Reducing Exceptions” at 6 (Nov. 11, 2013). The NACHA study does not give an average cost for small banks, but the un-weighted average for all banks is $100.52, so the average for smaller banks is undoubtedly higher than that. The weighted average for all banks, taking into account each bank’s volume, is $4.99.
New Technology May Come with Outdated Protection

Employers and government agencies are increasingly adopting prepaid cards instead of paper checks to pay unbanked workers and recipients of government payments. Prepaid cards, often Visa- or Mastercard-branded, have advantages for unbanked consumers but may fall into a loosely regulated gap in federal and state consumer protection laws.

Prepaid cards can come with high fees, including for withdrawing cash, checking balances, declined transactions, customer service, inactivity, overdrafts, and other items. The cards may provide no statements to check for unauthorized transactions or may require an unsophisticated individual with limited computer access to monitor transactions on the internet. Consumers may have little protection from loss of funds if an unauthorized charge is not disputed promptly, even if the consumer is unaware of the charge.

Congress, state governments and employers can remedy these problems through better laws or through negotiations with card issuers. The U.S. Treasury Department’s new Direct Express Card, aimed at 4 million unbanked Social Security and Supplemental Security Income recipients, is a relatively good model. Payroll or government benefits cards should have the following elements:

- **Choice and information.** Consumers should have the choice, before payments begin, to accept payments by direct deposit, by prepaid card, or by paper check, after receiving clear information about fees and other terms. Consumers should not have to opt in to direct deposit. Offering consumers choice gives prepaid card issuers the incentive to make their cards attractive to those without bank accounts.

- **Low fees.** Consumers should be able to obtain cash, get information, and perform basic functions with no fees. The Direct Express Card charges no fees for the following: participation (i.e. monthly fee); inactivity; purchases; the first ATM withdrawal per deposit (more would be better); deposits; unlimited bank teller withdrawals; ATM and telephone inquiries; low-balance and deposit phone, email or text alerts; overdrafts or declined transactions; ad hoc requests for a statement; customer service; one annual replacement card.
The law or provider agreement should prohibit any fees other than those expressly permitted.

- **Statements.** Prepaid cards can be subject to unauthorized charges, and recipients should be aware of any fees they are incurring. Paper statements should be available free or for a nominal fee (the Direct Express Card charges only $0.75/month). Statements should be automatically provided, as the default option from which recipients can opt out.

- **Free deposit and low balance alerts.** Cards should follow the Direct Express model of providing free deposit and low balance alerts by telephone, text message, or email.

- **Dispute rights and liability limits.** Congress or the Federal Reserve Board need to clarify that prepaid cards are entitled to full protection under the Electronic Funds Transfer Act. But liability for unauthorized charges should be capped at $50, as it is for credit cards, and the time to dispute a charge should not start running until the consumer receives a statement.

- **No overdrafts or payday features.** As with the Direct Express Card, overdrafts and overdraft fees should not be permitted, and there should be no fee for declined transactions.

- **Garnishment protection.** Any funds exempt from collection under state law (such as unemployment insurance or minimum bank balances in some states) should be protected from garnishment and freezing, as they are on the Direct Express card. The card issuer should be required to segregate exempt funds from any other funds on the card.

- **Wide acceptance and convenient access to free withdrawals.** The card should carry a widely accepted brand (i.e., Visa or MasterCard), should access a convenient network of surcharge-free ATMs, and should permit free cash withdrawals from teller windows and any point-of-service provider permitting cash back from a purchase.

- **FDIC insurance.** Payroll cards receive FDIC insurance, but other prepaid card funds are insured only if the account is structured properly.

- **Enforceability.** Cardholders should be able to enforce these rules in court if they are violated.

*Workers and other consumers* should look for ways to protect themselves. Though card terms vary, consumers may be able to take advantage of these features:

- **No-fee cash withdrawals** may be available inside at the teller window at Visa or MasterCard member banks (most banks) or as cash back from a purchase.

- **Sign up for statements, if available.** A small fee is worth it to be able to monitor charges and have a record of purchases.

- **Ask for deposit and low balance alerts,** which may be available by phone call, email or text message.
Electronic Payments in the U.S. Economy: An Overview

By Stuart E. Weiner

Business publications are filled these days with stories about the digital or electronic economy. One routinely reads about e-commerce, e-business, and e-banking. Terms such as e-mail and e-tickets have entered the common lexicon. Some analysts have gone so far as to proclaim that the U.S. economy is being fundamentally transformed and is entering a “new age” of unparalleled growth and opportunity.

While such a view is open to debate, clearly some major, potentially far-ranging, changes are under way. The most visible and most dramatic involve e-commerce. A growing amount of economic activity is taking place on the Internet, directly or indirectly impacting households and businesses throughout the economy. Less visible, but also significant, are changes involving “e-payments.” Although the U.S. payments system continues to rely heavily on paper-based methods, cash and checks, for conducting transactions, electronic payments are steadily gaining a greater presence.

This article provides an overview of e-payments as they currently exist in the United States. It shows that the U.S. payments system is becoming more electronic, principally through traditional means. While new instruments are beginning to emerge, it is the traditional e-payment types—credit cards, debit cards, and ACH transactions—that are driving the U.S. payments system forward.1

The first section of the article reviews cash and check usage in the United States, noting that even these instruments are becoming more electronic. The following sections then survey the various types of e-payments proper, including credit and debit cards, wire transfers and ACH transactions, and e-money. The article closes with a brief discussion of some of the factors that may influence the evolution of e-payments in the U.S. economy in the future.

I. CASH AND CHECKS

Cash and checks remain the dominant forms of payment in the United States. Even these paper-based instruments, however, are being affected by advancing electronic technologies.

Cash and ATMs

While the use of cash (currency and coin) is extremely difficult to measure, many estimates place its share at 50 percent or more in terms of the total number of transactions in the U.S. economy.2 Cash, of course, is inherently a non-electronic payments method. But its usage
in recent years has been bolstered, or at least sup-
ported, by a decidedly electronic dispenser, the
automated teller machine (ATM). ATMs do not
represent a payments type per se, but rather are
an electronic means of dispensing cash. They
offer a convenient alternative to more tradi-
tional dispensers, such as bank tellers, automo-
bile drive-through facilities, and supermarket
checkout lines.

An ATM card allows a customer to withdraw
cash from his or her bank account by entering a
PIN number and having the amount of the with-
drawal immediately debited from the account.
ATM transactions rely on an extensive commu-
ications system that includes both regional and
national networks that can interact with one
another. The four participants in an ATM trans-
action include the customer, the card-issuing
bank, the ATM owner, and the network or net-
works that the card-issuer and ATM owner join.
Outwardly seamless and quick, an ATM trans-
action in fact involves a series of complex,
underlying, interrelated processing steps.

The total number of ATM transactions has
more than doubled over the last ten years and is
estimated to reach near 11 billion again this
year. And although there are signs that ATM
volume may be peaking, ATM access continues
to grow. The total number of ATM terminals
has tripled over the last ten years (Chart 1).
Today, more than 50 percent are located off
bank premises at such locations as convenience
stores, gas stations, and shopping malls (*Bank
Network News*). Somewhat ironically, the
growth in ATMs and their ever-widening access
is contributing to the e-economy “feel” despite

---

*Chart 1*

**NUMBER OF ATM TERMINALS**

![Bar chart showing the number of ATM terminals from 1989 to 1999.]

being intrinsically linked to a core, paper-based payments method.

**Checks and ECP**

The other principal paper-based method, the check, also remains deeply embedded in the U.S. payments system. As shown in Table 1, 66 billion checks were written in the United States in 1997, accounting for 72 percent of the total number of noncash transactions. The United States utilizes checks more than any other industrialized country. But while check usage remains at an extremely high level, its share is trending downward (from 79 percent in 1993) as the growth in checks trails the growth of other, electronic, payments types. As noted in the table, credit cards, debit cards, ACH transactions, and wire transfers are all experiencing faster growth than checks, the result being that the sum of their transaction shares has risen from 21 percent in 1993 to 28 percent in 1997. Thus, e-payments are on the rise in the United States, and each of these payments types will be discussed shortly.

Still, checks remain pervasive in the U.S. payments system, used by individuals, businesses, and governments alike to pay for a vast array of goods and services. And, unfortunately, the clearing and settling of a check is an expensive process, estimated to cost two to three times more than an electronic payment (Hancock and Humphrey). A check accepted by a merchant, for example, must first be deposited at the merchant’s bank, sorted with other checks, and then physically transported to the payer’s bank for collection. Along the way, there are numerous processing steps, and the associated personnel, equipment, and transportation costs are high.

In recognition of this, clearing house associations, the Federal Reserve, and the banking industry in general have been striving in recent years to electronify various aspects of the check collection process. This effort is called electronic check presentment (ECP), a process by which the routing and payment information on a paper check is unbundled from the check.

---

**Table 1**

**NONCASH PAYMENT TYPES, UNITED STATES**

<table>
<thead>
<tr>
<th></th>
<th>Number of transactions 1997 (billions)</th>
<th>Average annual growth in number of transactions, 1993-97 (percent)</th>
<th>Share of number of transactions 1993 (percent)</th>
<th>Share of number of transactions 1997 (percent)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checks</td>
<td>66.09</td>
<td>2.3</td>
<td>79.1</td>
<td>72.2</td>
</tr>
<tr>
<td>Credit cards</td>
<td>16.88</td>
<td>7.8</td>
<td>16.4</td>
<td>18.4</td>
</tr>
<tr>
<td>Debit cards</td>
<td>3.91</td>
<td>53.3</td>
<td>.9</td>
<td>4.3</td>
</tr>
<tr>
<td>ACH</td>
<td>4.55</td>
<td>15.5</td>
<td>3.4</td>
<td>5.0</td>
</tr>
<tr>
<td>Wire transfer</td>
<td>.15</td>
<td>7.3</td>
<td>.1</td>
<td>.2</td>
</tr>
</tbody>
</table>

itself and transmitted electronically to the paying bank. In the strong form of ECP—known as truncation—the paper check never follows. In the weak form of ECP, the paper check is eventually sent to the paying bank, negating some of the cost savings that would result from full truncation but still making the check collection process faster and more efficient. Over the first seven months of this year, 18 percent of the total checks processed by the Federal Reserve were presented electronically, either in truncated form or with checks to follow.

As part of the ECP effort, other programs are also under way that are designed to bring advanced technologies to check clearing and settlement. Some Federal Reserve offices, for example, are now offering pilot programs that offer digital images of truncated checks to ECP customers over the Internet. The use of digital imaging in other parts of the check process is being explored as well. Thus, as with cash and ATMs, there is a growing “electronic” aspect to checks. But in all such check electronification programs, a paper check still enters the system. The mark of a true electronic payments type—an e-payment—is no paper. E-payments are taken up next.

II. CREDIT CARDS AND DEBIT CARDS

The first major category of electronic payments is credit cards and debit cards. Together, they account for nearly a quarter of noncash transactions in the U.S. economy.

Credit cards

Credit cards are the most common and most familiar e-payment type in the United States. As shown in Table 1, there were nearly 17 billion credit card transactions in 1997, representing 18.4 percent of all transactions. Over the 1993 to 1997 period, credit card transactions grew at a 7.8 percent annual rate.

Credit card transactions take place over large electronic networks, typically linking cardholders, merchants, card-issuing banks, merchants’ banks, and the credit card companies. Roughly half a billion general purpose cards are in circulation, with 85 percent of those being bank-issued MasterCard or VISA cards. But nonbank general purpose cards—American Express, Discover, and Diners Club cards—also play an important role, presently accounting for over one-fourth of all general purpose dollar outlays (Nilson Report 1999).

Some of the recent growth in credit card transactions no doubt reflects the increase in purchases of goods and services over the Internet, that is, e-commerce. Although definitive data are lacking, available information suggests that a large majority of Internet purchases are currently conducted via credit card. Some card-issuing banks are aggressively seeking to grow their Internet-related business, urging customers to choose their particular credit card for online purchases. Other card-issuing banks are viewing the Internet more as a marketing tool, using online advertising to entice new customers to apply for their card. Reflecting both strategies, cobranding of bank credit cards with Internet firms is on the rise (American Banker).

Credit card usage for Internet sales has also spurred discussion of so-called digital wallets. One of the drawbacks of using credit cards for online purchases is that credit card information, as well as billing and shipping information, has to be reentered into a form every time a new merchant is visited. A digital wallet is software that permits the cardholder to store such information on his or her personal computer or on a server operated by the company issuing the wallet. When the customer is ready to make an online purchase, he or she can transmit these data with a single mouse click, making Internet credit card transactions easier. To date, however, digital wallets have attracted little interest from consumers.
Debit cards

While credit cards remain the principal type of electronic payment in the United States in terms of the number and share of transactions, the use of debit cards is growing at a much faster rate. Indeed, debit cards are the most rapidly growing payment type in the United States. As seen in Table 1, annual debit card transaction growth has averaged 53 percent in recent years, and debit cards now account for over 4 percent of total transactions. The number of debit cards in circulation has reached some 250 million (Bank Network News). A recent Federal Reserve Bank of Kansas City survey reflects these trends: 77 percent of responding banks now offer debit cards, and an additional 14 percent plan to do so within a year.

Debit cards are used for point-of-sale (POS) transactions; that is, a customer presents a debit card to a merchant just as he or she would present a credit card. But debit card transactions do not involve credit. Instead, as with ATM transactions, debit card transactions are linked to a customer’s bank account. Online debit transactions require the customer to enter a PIN number, and the amount of the transaction is immediately debited from the customer’s account. Offline debit transactions require a signature, and, while settlement is not immediate, authorization is required.

Like ATM and credit card transactions, debit card transactions are made possible through interlinked communications networks. Participants include consumers, merchants, card-issuing banks, merchants’ banks, and regional and national networks. Online debit card transactions operate through the same networks as ATM transactions. Offline debit card transactions operate through credit card networks. A typical debit card will allow the holder to access one or more debit card networks as well as one or more ATM networks.

A number of factors have likely contributed to the increased use of debit cards in recent years. Growing familiarity with the debit card instrument, increased consumer and merchant acceptance, more aggressive marketing on the part of banks, and the convenience of coupling POS and ATM capabilities on a single card have probably all played a role. Another key factor has been the emergence of the VISA and MasterCard offline debit card networks, which piggyback off their respective credit card networks. Introduced in the early 1990s, these networks have opened up the entire VISA and MasterCard credit card infrastructures to debit card users.

Reflecting this, while the number of online debit card transactions has been rising sharply, the number of offline transactions has surged even more. Since 1995, offline transaction volume has grown at a 60 percent pace (Bank Network News). The number of offline debit cards in circulation has nearly tripled (Chart 2).

In addition to their standard uses, debit card networks and ATM networks are also being used for Electronic Benefits Transfer (EBT) programs. These programs are being used by various government agencies to deliver cash entitlement and food assistance benefits to recipients who do not have bank accounts. Recipients are issued cards that allow them to make cash withdrawals from designated ATM machines or to make food purchases at the debit card terminals of designated grocery and convenience stores. At present, the federal government and 39 states have EBT programs in place, providing benefits to over 4 million families (Federal Electronic Commerce Program Office).

III. WIRE TRANSFER AND ACH

A second major category of electronic payments is funds transfer systems. Unlike credit and debit cards, which place a payments instru-
ment in the hands of the user, funds transfer systems are entirely instruction-driven. Two types of funds transfer systems operate in the United States, wire transfer and ACH (Automatic Clearing House).

**Wire transfer**

Wire transfer transactions are high-value, “wholesale” payments that are made among banks and other financial institutions. As shown in Table 1, wire transfers account for less than 1 percent of transactions in terms of volume. However, they account for a very large share of transactions in terms of dollar value.9

Wire transfers are conducted over two electronic payments networks, Fedwire and CHIPS (Clearing House Interbank Payment System). Fedwire is operated by the Federal Reserve System and is used to settle interbank transactions. CHIPS is operated by the New York Clearing House Association and is principally used to settle foreign exchange transactions. The average size of a Fedwire transaction is currently about $3 million, while the average size of a CHIPS transaction is about $6 million (Gramlich).

**ACH**

ACH funds transfers, in contrast, are typically much lower in value, currently averaging about $3,000 (Gramlich). As such, they are closer in function to the other “retail” instruments, that is, cash, checks, and credit and debit cards.

---

The ACH network is a nationwide electronic payments system in which payment instructions are exchanged among participating financial institutions acting on behalf of consumers, businesses, and governments. In existence since the early 1970s, the network is used for such transactions as payroll deposits, automatic bill payments, and corporate tax payments. It also is often used as the underlying settlement mechanism for other transaction types, including ATM, credit card, and debit card transactions. According to industry estimates, 20,000 financial institutions, 2 million businesses, and 100 million consumers directly or indirectly use the ACH network (NACHA 1999c).

As seen in Table 1, ACH is the second-fastest growing payment type in the United States, growing at a 16 percent annual rate in recent years. Like debit cards, however, its share of overall transactions remains relatively small, currently 5 percent.10

An ACH transaction involves a number of parties. At its root is an “originator”—an individual, business, or government—electronically transferring funds to (credit) or from (debit) the bank account of another party, the “receiver.” Originators and receivers gain access to the ACH network through financial institutions. Financial institutions, in turn, use a central clearing facility—an ACH “operator”—to process, distribute, and settle transactions. There currently are four ACH operators in the United States. The largest is the Federal Reserve, which clears approximately 80 percent of all ACH transactions.11

As noted above, the ACH network is used for a variety of transactions. Most familiar, perhaps, are direct deposit transactions, in which individuals have their salary pay or government benefits directly deposited into their checking or savings accounts. Roughly 50 percent of employees now participate in payroll deposit programs, for example, and 75 percent of social security recipients now receive their benefits electronically.12

A second way in which many individuals and households use the ACH network is to make automatic, recurring bill payments, such as mortgage and utility payments. Bill payments and other consumer debits generated 1.2 billion ACH transactions in 1998, a 17 percent increase from a year earlier (NACHA 1999b).

Businesses also use the ACH network extensively. In addition to offering payroll deposit programs to employees, many businesses use ACH to pay suppliers and contractors electronically. Some businesses, particularly large retailers, use the ACH network to consolidate funds received at dispersed locations. And a growing number of businesses are also making corporate tax payments via ACH.

The third major originator of ACH transactions is the federal government. Currently, 73 percent of all U.S. Treasury-disbursed payments are conducted electronically, including 96 percent of payroll payments, 73 percent of benefit payments, and 50 percent of vendor payments (U.S. Department of the Treasury, Financial Management Service). In keeping with the goals of the Debt Collection Improvement Act of 1996, the federal government has been actively promoting use of electronic payments under the EFT 99 umbrella program.

The ACH network is of interest not only because of current activity but also because of prospective activity. Two emerging payments vehicles, electronic bill presentment and payment (EBPP) and POS check conversion, are receiving increased attention from consumers and businesses. Both are ACH-related.

*Electronic bill presentment and payment.* EBPP is a way for consumers to receive and pay bills on the Internet. EBPP has two components—electronic bill payment and electronic bill presentment. Electronic bill payment is already a reality. Numerous providers, both banks and nonbanks, currently offer bill-payment ser-
vices in which customers who have received bills in the mail can contact the provider by telephone or personal computer to initiate payments. Where possible, payments are made through ACH transactions; otherwise, they are made by check. Use of electronic bill payment is becoming more popular, reportedly doubling in 1997 from a year earlier (Furst and others).

EBPP combines electronic payment with electronic presentation; that is, it brings bills online to the consumer. The consumer is able to access his or her bills online and then to pay online. Two principal models are being developed for doing so. In the first, the Biller Direct model, the billing firm (say, a utility) makes its bill available to the consumer at the firm’s web site. The consumer accesses the bill and pays it via ACH or credit card. The drawback is the consumer has to visit the web sites of all billers. In the second model, the Consolidator model, some third-party “presenter” collects bills from a number of billers and makes them available to the consumer at a central site. In this case, the customer only has to visit, and pay bills, at that one presenter’s web site. EBPP is still in the development stages, but it is getting a good deal of attention.

Check conversion. The same is true of POS check conversion. This is a process by which a paper check is converted at the point of sale into an ACH transaction. A customer presents a blank check, which is scanned for account information. The check is then stamped void and either given back to customer or kept by the merchant. Either way, a paper check never enters the system. POS check conversion has been tested at approximately 1,700 pilot locations and is beginning to be offered by some major retailers (Chain Store Age).

In a similar vein, some Internet sites are offering what might be called online check conversion. This vehicle is similar to POS check conversion in that the customer first provides check information, and then the transaction is converted to an ACH transaction. Like its POS counterpart, however, such transactions are just starting to be used.

IV. E-MONEY

Another class of emerging e-payment instruments might be grouped under the term “e-money.” Although most of these have generated only limited consumer and merchant interest to date, and sketchy data preclude an entry in Table 1, the group includes some innovative and potentially important payments mechanisms.

Stored-value instruments

One type of e-money is prepaid stored-value products. Funds are stored in electronic form on either cards—"stored-valued cards"—or on computers—"e-cash." Stored-value cards can be either multipurpose (open-system) cards that are used to make a variety of payments or single-purpose (closed-system) cards that are used more narrowly. E-cash products are typically multipurpose in design.

There are numerous examples of single-purpose stored-value cards. These include mass transit cards, telephone cards, photocopying cards, and electronic gift certificates. The use of such cards appears to be growing, but an accurate count is difficult to obtain because of the lack of comprehensive data.

Far less prevalent are multipurpose stored-value cards. Such cards, which typically employ “smart card” technology by embedding a computer chip in the card itself, have not gained much acceptance in the United States. The conceptual advantage of such cards—wide applicability—is also a disadvantage. For such a system to be successful, a large number of merchants must be willing to incur the costs of installing associated hardware. Some European countries, in contrast, have seen somewhat greater acceptance of multipurpose cards.
E-cash products have also had little impact in the United States. Such products may entail installing software on consumer and merchant computers that allows some type of “digital coin” to be exchanged. An early, unsuccessful example was a program developed by DigiCash, Inc., in which a participating bank could issue e-cash—a string of electronic digits—to depositors, who in turn could use this e-cash to make online purchases at participating merchants. A current example is a program developed by Flooz.com, in which a consumer purchases (via credit card) units of an electronic currency called “Flooz,” which in turn can be spent online at participating merchants. To date, however, the adoption of such instruments has been very limited.18

Micropayments and e-checks

An e-cash system provides one way to make “micropayments” on the Internet, that is, to accommodate payments that are too small for credit card purchases. Other types of micropayments are also being explored. One involves billing through Internet service providers (ISPs). Participating merchants send purchase information to a customer’s ISP, which adds it to the customer’s monthly ISP bill. Another involves billing through a customer’s telephone company.19 Micropayment approaches like these in some sense represent a new variant of e-money.

A final type of e-money is the “eCheck,” a payments instrument that has been developed by the Financial Services Technology Consortium, a group of banks, government agencies, and other financial industry participants. The eCheck is modeled after the paper check, but it is completely electronic. Each step of the process—writing, delivering, depositing, clearing, and settling the check—is done electronically. Because the eCheck is designed to be robust enough for use on the Internet, it uses advanced security technologies. A different instrument than the check conversion products described earlier, the eCheck is currently being tested on a limited basis by the U.S. Treasury Department.20

V. CONCLUSION

The U.S. payments system is becoming more electronic. As this survey has shown, all major types of e-payments are trending upward, and some new electronic payments instruments are beginning to emerge. While the United States still substantially lags behind other industrial countries, its use of electronic payments is rising.

Clearly, checks remain the preferred form of noncash payment in the United States. From a consumer’s standpoint, checks possess several attractive features. They are familiar, widely accepted, relatively convenient, and they give the user hands-on “control” over a given payment. Most important, checks, like cash, enable individuals to make payments to other individuals. No other single, competing electronic method presently offers the same mix of attributes. In addition, banks and other financial organizations have committed heavy resources to the check collection process and have an incentive to support it as long as their customers are demanding it.21

Multipurpose stored-value instruments, in particular, have been slow to catch on in the United States. One reason—and one that typically factors into the adoption of any new payments mechanism—is cost. An e-money system may require an investment in equipment and staff that merchants are unwilling to bear until they are convinced that customers will be interested. Customers, in turn, may not be interested in an e-money system until enough merchants are participating. Reaching this critical mass of users is a hurdle that any almost new payments mechanism has to overcome.22 A second factor that may be contributing to the slow growth of e-money instruments is uncertainty over security, standards, and compatibility issues
associated with the new technologies. And a third reason may be the growing popularity of alternative, more “traditional” e-payments types, including debit cards and various ACH products. As the volume shares make clear, traditional e-payments have become an increasingly important component of the U.S. payments system.\(^2\)

Indeed, the U.S. payments system is becoming more electronic principally through traditional means. Existing e-payment types—credit cards, debit cards and ACH transactions—are accounting for a rising share of U.S. transactions. More novel e-payment types have yet to have much impact.

Looking ahead, there are reasons to believe that the trend toward greater electronification will continue. First, the dramatic rise in e-commerce should provide the impetus and synergies for increased online transactions. Second, the shift in demographics toward a young-adult group that came of age in the high-tech 1990s may make the average household more comfortable with electronic payments of all kinds. Of course, it is difficult to foresee with any certainty how quickly and in what forms electronic payments will evolve in the U.S. economy. One of the defining characteristics of the new digital economy is its dynamic—and unpredictable—nature.

**ENDNOTES**


2 See, for example, Hancock and Humphrey, and Humphrey and Pulley.

3 By comparison, checks’ share of the total number of non-cash transactions, in 1997, for various other countries was: France, 41.7 percent; Canada, 36.1 percent; United Kingdom, 30.5 percent; Belgium, 8.0 percent; Germany, 5.7 percent; and Netherlands, 3.0 percent (Bank for International Settlements 1998).

4 While credit cards are almost always treated as a payment type, analogous to cash, checks, and other instruments in facilitating the purchase of goods and services, they also possess a consolidation feature. A monthly credit card balance—which itself is paid for through some other means—represents, of course, the consolidation of a number of individual transactions.

5 Credit card processing was not always electronic; at one time, it was heavily paper-based.

6 A third group of credit cards, private-label cards for use at specific retailers (for example, department stores and oil companies) accounted, in 1997, for about 17 percent of overall credit card dollar volume (Nilson Report 1998).

7 Robert Powell of VISA and David Weisman of Forrester Research, for example, have reported such at recent industry conferences.

8 For further discussion, see Electronic Consumer News 1999b and Nilson Report 1999.

9 Dollar-value shares in 1997 for the various payments types were: wire transfer, 87.49 percent; checks, 10.46 percent; ACH, 1.88 percent; credit cards, .14 percent; and debit cards, .02 percent.

10 Although ACH transactions are subject to some double counting, industry sources estimate that such is extremely small, on the order of .4 to .6 percent in 1998.

11 The other three operators are the Electronics Payments Network (EPN), American Clearing House Association, and VisaNet ACH.

12 The payroll deposit figure is based on Mid-America Payment Exchange and Gramlich. The Social Security figure is taken from U.S. Department of the Treasury, Financial Management Service.

13 Another option might be for the presenter to send the bills to the consumer via email.

14 For further discussion, see Furst, Lange, and Nolle.

15 Past U.S. experiments include the 1996 Olympic Games in Atlanta and 1997-98 pilot programs in New York City (Gramlich).
16 Multipurpose stored-value cards could also potentially be used to transfer funds between individuals.

17 Belgium, Germany, the Netherlands, Sweden, and Switzerland, for example, currently operate low-volume national systems (Bank for International Settlements 1999).

18 For further discussion of stored-value instruments, see Gramlich, CNNfn, Bank for International Settlements 1999, and O-Mahoney, Peirce, and Tewari.

19 For further discussion, see Electronic Commerce News 1999a and Bransten.

20 The eCheck instrument is described more fully in Financial Services Technology Consortium and Marjanovic.

21 The role of checks in the U.S. payments system is examined in U.S. General Accounting Office (see especially p. 175), Humphrey and Pulley, and American Bankers Association. See also Grippo for a discussion of peer-to-peer transactions.

22 This phenomenon of a new payments mechanism taking on more value to existing users as more users elect to participate is an example of “network economies.” For discussion, see Craig, Gramlich, and Bank for International Settlements 1999.

23 Gramlich and Bank for International Settlements 1999 offer additional thoughts on some of these points.

REFERENCES


Role and Security of Payment Systems in an Electronic Age

Remarks Prepared for
IMF Institute Seminar on
“Current Developments in Monetary and Financial Law”

June 1, 2004

by

Mark Fajfar*
Fried, Frank, Harris, Shriver & Jacobson LLP

In the past decade, methods of effecting banking and other financial transactions via the Internet in the United States have quickly become more and more sophisticated. This paper will examine, from the viewpoint of a U.S. legal practitioner, the implications of this trend towards conducting financial transactions electronically. The focus of this paper is not on legal theories, but rather on the interesting and novel practical issues that arise in the legal implementation of new electronic payment systems that are now more prevalent or are appearing on the horizon. This paper discusses consumer, as opposed to business-to-business, transactions and concentrates on how the particular characteristics of the new electronic payment systems (contrasted to the “traditional systems”) affect the consideration of two issues: information security and efforts against money laundering and terrorist financing.

A “silent revolution” in the payment systems in the U.S. has occurred over the past decade or so. Payment systems are moving from paper towards real-time, electronic execution and settlement. “Real-time” means that payments are settled or cleared not

---

* This paper reflects only the author’s own views, not the views of Fried Frank or any of its clients. The author recognizes Fried Frank’s Financial Institutions and Electronic Commerce Transactions Group, headed by Thomas P. Vartanian and including Robert H. Ledig and David L. Ansell, for their contributions to this paper.
only in a few days or even overnight, but on a continuous basis, 24 hours a day. Consumers have generally been willing to adopt these new electronic systems because they have confidence in the financial system in general and in electronic operations in particular. But this is a silent revolution because these extensive changes have occurred slowly, and not necessarily in ways that are obvious or dramatic. The traditional, trusted and convenient means of effecting payments still have a strong attraction to consumers, who therefore change their economic behavior slowly because of their emotional relationship to money and the payment mechanisms they trust.

Overview of New Electronic Payment Systems

Before talking about the security and law enforcement implications of the new payment systems, this paper will briefly describe the new systems themselves. As a preliminary aside, the reader should note that this paper does not discuss the credit and debit card systems in detail, for two reasons. First, credit and debit cards are so pervasive a means of effecting electronic transactions in the U.S. that a discussion of them would at least double the length of this paper. Second, this paper aims to address recent changes in the electronic payment systems and the implications of those changes on the issues of information security, money laundering and terrorist financing. While they are important, the credit and debit card systems are not especially changing at this time (and to the extent they are, this paper will discuss them). Nonetheless, the credit and debit card payment systems are a crucial part of the overall U.S. consumer finance structure, and much of this paper’s discussion of information security and other concerns does apply to credit and debit cards.

Transformation of the Paper Check

The silent revolution in payment systems in the U.S. is most apparent in the ongoing transformation of the paper bank check, which has been for decades the mainstay of the consumer payment system. The demise of the paper check has been predicted since at least the 1960s, but its familiarity, simplicity and consumer protections
have fostered its continued use, and a very large percentage of payments are effected today by paper checks.

Electronic processing of check transactions has accelerated, however – the primary change being the increasing use of the automated clearing house (“ACH”) system for direct deposits and direct payments. Common uses are the direct deposit of payroll checks and consumer payment of recurring bills by direct payments to utilities, for example. Furthermore, these systems are evolving into a comprehensive system of electronic bill presentment and payment, which permit a consumer to register (typically through a bank, but also through third-party service providers) to receive bills from a variety of merchants by electronic mail, rather than postal mail. Then, instead of using checks, the consumer uses the Internet to initiate direct electronic payments to those merchants.

The important lesson from the transformation of the paper check is that it reflects a gradual expansion of an electronic system. In the early stages, the ACH system was used for only repetitive payments to specific merchants. Today, this electronic system encompasses the billing process and payments to a variety of merchants.

There is also much discussion today of the Check Clearing for the 21st Century Act, Pub. L. No. 108-100, 117 Stat. 1177 (2003) (“Check 21 Act”), which will permit “electronic check truncation.” That is, banks will be permitted to convert paper checks to electronic entries, and process the check transaction electronically, without the physical delivery of checks from place to place.

Electronic Payment of Government Benefits

Another new application of electronic payment systems is their use to provide government benefits. Already, federal, state and local governments favor the ACH direct deposit system for payments to individuals – such as tax refunds, social security benefits and cash assistance. While that system is relatively straightforward, difficult issues arise
when governments seek to make electronic payments to people who do not have bank accounts (which constitute a significant number of lower-income individuals). For them, the existing, paper check-based system imposes costs on both the government-payor and the recipient. The government has to pay for the printing and mailing of checks, and the individual recipient has to pay the cost of a check cashing service.

For this reason, governments have started to pay benefits in the form of debit cards known as electronic benefits cards. These are similar to cards used at automated teller machines (“ATMs”). The electronic benefits cards are periodically “loaded” with additional funds by the government (i.e., the government deposits funds into a bank account tied to the cards). Individuals use the cards to make purchases in stores or to withdraw cash from ATMs.

The interesting point here is that the large volume of government payments is likely to hasten the acceptance of debit cards as a means of transferring funds to individuals. Similar systems are sometimes used for payroll, especially the payment of wages to transient or temporary workers. The issue discussed later in this paper is whether, as the use of debit cards to transfer funds to individuals becomes more common, they could also be used for money laundering or terrorist financing.

**Person-to-Person Electronic Payment Systems**

The previous two examples are illustrations of the evolution of an existing system into a new, electronic format. In addition, other electronic payment systems have introduced entirely new ways to transfer funds between individuals.

For example, person-to-person electronic payment systems, such as PayPal, are used to transfer funds electronically among individuals without using cash or checks. Basically, these systems require that each user designate a bank account or a credit card account. Then, when an individual initiates an electronic transfer to another, PayPal’s
An electronic system causes a debit in the account of the payor and a credit in the account of the payee.

Many similar systems were introduced during the technology boom of the late 1990s. Those that remain viable found success in niche markets, such as facilitating purchases between individuals on Internet auction sites like eBay. The advantages of these systems are that they clear payments faster than check processing systems, do not impose the high fees of credit cards, and do not impose merchant-qualification requirements. Instead, anyone with a bank account or credit card can use a PayPal account to receive money electronically from other individuals.

“Closed-System” Stored Value Cards

A wide variety of new electronic stored value cards which defy easy classification under traditional rules and regulations have recently appeared. For example, electronic gift cards issued for a particular value by a particular merchant have become very popular. The card can be given as a gift, or just used as a convenient way to make purchases at the merchant later on. Ease of use and convenience are the primary attraction of these cards to consumers, while merchants favor them because customers tend to spend more freely when using a gift card (probably because of the disconnection between the payment of money and the use of the card).

Similar cards are issued by the larger urban mass transit systems, universities and other “campus-based” organizations to permit users to make payments within the issuing system. Typically, the consumer loads a certain amount of money onto the stored value card (using cash or a credit or debit card) and then spends that amount over time. The Washington area Metro uses an electronic stored-value card, for example, and the EZ-Pass and other systems for toll roads are prevalent in large cities throughout the U.S. All of these systems are primarily for relatively low value transactions. They are called “closed-system” stored value cards because their use is usually limited to a single merchant or organization.
“Open” or “Universal” Stored Value Cards

“Open” or universal electronic stored value cards – that is, those that can be used at a large number of locations of diverse types – have so far failed to succeed in the U.S. because there simply does not appear to be demand for a new electronic alternative to cash. The existing credit card, debit card and ATM systems already meet this demand, since they are convenient, inexpensive and widely available.

“High Velocity” Payment systems

Looking to the future, however, the new systems we anticipate will likely succeed could be called “high velocity payment systems.” Private or quasi-public electronic payment networks, such as highway toll pass and urban mass transit fare pass cards, are becoming more sophisticated and being used by more consumers. Similarly, some merchants are attempting to expand the use of stored value cards they issue. In some trials, these cards can be used at a wider variety of locations. That is, they are transforming from closed systems to open systems. Mobile telephone service providers are entering the field with nascent offerings which may yet overcome the lack of industry standards and other practical challenges.

These systems are designed to be transparent to the consumer, and their focus is on repetitive, low value payments where speed and convenience are the primary goal. The twist they add to the merchant-specific cards is that they hope to offer consumers the ability to make payments at a wide variety of locations. It is likely that in the near future these products will add more features and expanded functions in order to be more widely accepted. In doing so, they face the same challenges that faced Mondex, CyberCash, DigiCash, and other systems in the 1990’s.

Acceptance of Electronic Payments in U.S. Financial System

The issue in all the new electronic payment systems described above – the problem they all face – is whether and how they will effectively replace all the functions
of the paper cash and check systems, including their familiarity and acceptance by consumers. In thinking about this issue, it is helpful to consider two particular characteristics of the U.S. financial system which have affected how electronic payment systems have been implemented and gained acceptance to date.

The first important characteristic of the U.S. payment systems is that they are, as a practical matter, regulated not only by government laws and regulations, but also by the internal rules of private organizations, which apply to the settlement of checks, credit cards and other payment devices. That is, banks and merchants agree on a voluntary basis to abide by the rules of, for example, the National Automated Clearing House Association ("NACHA"), which governs check processing, and the rules of Visa, MasterCard, American Express and Discover, the main credit card organizations. These rules are, in turn, imposed on consumers when they agree to the terms and conditions of a bank account or credit card account which is governed by the rules.

For example, the rules of these private organizations resolve disputes regarding which party is liable for unauthorized transactions, or for authorized transactions that are not completed due to some error. For the large part, these rules provide that the consumer is not liable for unauthorized or erroneous transactions, which of course makes these systems more attractive to the consumer. The widespread acceptance by all parties (consumers, merchants, financial institutions and regulators) of the compromises reflected in these rules is one of the strengths of the currently predominant systems.

The second important characteristic of the U.S. payment systems is that they have not experienced any large or systemic failure within the past generation. While there have been scandals such as the savings & loan failures in the 1980s and the recent corporate accounting and governance scandals, neither have involved large scale losses to consumers. Similarly, the financial system recently withstood the Y2K problem and the September 11th attacks. Therefore, it is safe to say that U.S. consumers generally have a
high degree of confidence in banks, credit cards and electronic payment systems, and therefore are willing to try new systems as they are offered.

**Can New Systems Effectively Replace Paper Systems?**

Because of these two characteristics of U.S. payment systems, the operational challenge for the new electronic payment systems is to develop and maintain a private system of rules which replicates all of the functions of the traditional payment systems and also provides advantages over them. Over the long run, we believe the new systems will reduce costs and increase efficiency, but the short-term price may be some confusion in the absence of ground rules which are well-understood by consumers, businesses, financial institutions and regulators. The competition between the different systems to develop fair and effective rules is likely to benefit all parties involved rather than being a race to the bottom. In any case, it is clear that wider acceptance of the new payment products will require the development of universal standards, technologies and rules, which has not occurred yet.

From a legal perspective, the fundamental issue that the appearance of new alternatives to the traditional payment systems has raised for governments and financial regulators is the question of whether it is feasible to allow a mix of divergent commercial organizations to each have an effect on the nation’s payment system – i.e. its “money.” Before the appearance of new and, to some extent, less regulated electronic payment systems in the 1990’s, regulators did not have to ask themselves this question. To the extent they pay attention to this issue now, there is a possibility that laws will be changed to accommodate the new systems.

**Information Security and Money Laundering and Terrorist Financing**

The specific challenges the remainder of this paper will address are how the new payment systems will deal with the issues of information security and money laundering and terrorist financing.
We believe that information security aspects of the new electronic payment systems will, for the next few years at least, be an area of increasing concern to consumers, merchants, financial institutions and regulators. In this context, the term “information security” refers to efforts to protect electronic payment systems from the relevant threats.

On a basic level, what are the threats that are of concern?

- That an individual will break into an electronic system in order to initiate unauthorized transactions on another individual’s legitimate account, thereby stealing money.
- That an individual will steal customers’ personal data, enabling the wrongdoer to set up illegitimate credit card accounts, bank accounts and other accounts – this is called identity theft.
- That an individual will attack or corrupt the data in the electronic system, either as vandalism or to extort money from the sponsoring financial institutions.
- That an individual will take advantage of the convenience and speed of the electronic system to mask illegitimate or illegal transactions – i.e., money laundering.
- That an individual will take advantage of the efficiency of the electronic system to facilitate funding of illegal activities, particularly terrorism.

It is also useful to consider not only these specific threats, but also the underlying themes that are of particular concern in recent years. Three such themes are terrorism, identity theft and internal fraud (that is, fraud committed by employees or other “insiders” in the organization).
Systemic Measures to Secure Electronic Payment Systems

Obviously, sophisticated electronic systems and technical procedures exist which can be used to counter each of the threats mentioned above. But from a legal perspective, the primary area of concern is not the technical details, but instead the measures taken at a systemic level by financial institutions and other organizations to protect their electronic payment systems. Lawyers look at the security system as a whole in order to understand the framework in which these security measures will be evaluated. Lawyers focus on the fact that, at some point, a third party will examine the merchant or financial institution to determine whether its electronic payment systems are sufficiently secure. This third party could be a bank regulator conducting a periodic examination, or an independent auditor, or an adverse party in litigation, or an internal investigation conducted by the organization itself. The point is to consider, now, the factors which will be important in that examination, later, and to consider steps the organization should take, now, so that its systems will be in compliance, later. Lawyers cannot wait for a problem to occur in order to attempt to fix it.

Electronic Payment Systems Require Remote Interaction

The analysis of information security requires an understanding of the underlying characteristics of electronic payment systems which increase their vulnerability to security threats. For example, it is important to understand that remote interaction is crucial to electronic payment systems. At its core, any electronic payment system is based on an ability to query a database of financial information from a distance, and then cause that database to be modified (e.g., by making debit and credit entries) to reflect a transaction. But this remote interaction is also the characteristic which renders electronic payment systems vulnerable to fraud, hacking and other disruptions. This risk is becoming of greater concern as users demand continuous access to their funds and ever faster transaction completion.
Consider the practical implications of this remote interaction:

- In the traditional systems, financial transactions were initiated and completed by bank personnel, using proprietary systems located at the bank. Network connections to other banks occurred, but were the exception more than the rule. Many transactions were cleared based on paper documents (such as a check), with a higher degree of oversight by a human being.

- Currently, we are in the midst of rapid changes in these systems:
  - Financial transactions are initiated and completed by customers themselves, using computers that are connected to the bank’s systems via the Internet. This can include very high value transactions.
  - Network connections between systems of different banks are pervasive and virtually constant. Moreover, the U.S. financial system as a whole is dependent on these connections.
  - Fewer and fewer transactions are cleared on a paper basis. And virtually no high-value transactions are paper-based.
  - There is less and less human oversight of computers which clear transactions. That is, such operations are becoming more and more automated as the computer hardware and software becomes more sophisticated and autonomous.

**Steps to Information Security Compliance**

What are some of the steps that are recommended to secure electronic payment systems, in light of these changes and the resulting threats to the system? We refer to these steps as “information security compliance.”
• **Security efforts must be “risk-based,”** meaning that the company or financial institution must evaluate the threats to its information assets and concentrate on counteracting those that involve the highest risk of severe adverse consequences.

• **Security efforts must be continuous.** Compliance measures must be periodically tested, reevaluated and modified to maintain their effectiveness. For example, errors may arise when a company or institution hires new employees, opens a new branch or enters a new business without updating its security controls to account for the new activities. Similarly, when employees leave, branches close or businesses wind-up, the information systems devoted to those past activities must be properly cleansed.

• **Security efforts must cover the entire organization.** Specific practices and the compliance culture must be overseen by the board of directors and extend to the lowest level of employee with operational responsibility. In particular, the compliance program must take into account that “human error” (whether negligence or willful misconduct) is the greatest threat to information assets. There must be rigorous training of employees.

• **Information systems must permit later auditing in order to detect efforts to alter or compromise information.** Just as the “black box” is crucial to the investigation of a plane accident, there must be some means of reviewing how the information systems have actually been used and what they have actually done. If not, the organization will be unable to determine whether information security breaches have occurred, let alone determine how to prevent them.
• Third-party service providers must be held to the high standards. Many information systems tasks are subcontracted (or “outsourced”) to third party service providers which are able to perform these services more efficiently. But responsibility for information security cannot also be subcontracted. On the contrary, these arrangements require close attention to the subcontractor’s performance. In particular, the subcontractor should be subject to a written obligation that it meet all of the information security compliance standards of the hiring company or financial institution.

Manage Information Security as Part of Overall Legal Compliance

Last, and most important, it must be understood that the goal is not to create a list of compliance steps, and then conclude that if each of those actions is completed, the electronic system will be sufficiently secure. Instead, electronic payment systems need to be made secure as part of the organization’s overall legal compliance effort. For example, decisions about what specific hardware or software measures to take need to be made in a rational way and documented, so that when the security of the system is later examined by a regulator or third-party, the institution will be able to explain why it took the steps that it did, and did not take other steps. This cannot be haphazard. Similarly, it is important to maintain access controls and logs, so that it is possible to examine how the system is used – to understand, for example, how a security breach occurred, to what extent information was compromised, and so forth. Even the most up-to-date security systems are much less valuable if there is no record of how they were installed, how they have been operated, and how they may have failed.

Money Laundering and Terrorist Financing

Turning now to money laundering and terrorist financing concerns, and recognizing the difficulty of covering all facets of such a broad topic, this paper will instead consider how these concerns are implicated in the new electronic payment systems.
It is helpful to begin with a simple example.

- An individual in the United States can open a bank account over the Internet, generally by providing a name, social security number and address, without entering a bank office.

- The individual could then transfer any sum of money into the account electronically. Money could be transferred from the U.S. or from overseas.

- Using the account, the individual could purchase stored value cards offered by credit card systems and others, and mail those cards overseas.

- Persons in other countries, then, who let us assume would be prohibited from opening a bank account in the U.S., could use the cards to purchase goods and services using funds in a U.S. bank account. (The important question of whether use of the stored value cards would require the presentation of identification is a question of local regulation and practice.)

- Similarly, persons overseas could access cash in the U.S. bank account overseas by using an ATM card linked to the account, which typically does not require the presentation of identification.

What are the facets of this example that are unique to the new electronic payment systems?

- The first point is that as stored value cards gradually become more prevalent, common and accepted, their use becomes routine and does not draw attention.

- The second point is that none of the individuals involved in the example described above would have any interaction with a bank employee. So
there is no question of a bank employee “noticing anything suspicious” about them, the account or the transactions.

- The third point is that in this example, an electronic network is the crucial “choke point.” That is, since there is no person-to-person interaction, we must rely on an electronic computer network to detect illegal activity. Presumably, the bank or credit card networks involved in the transactions would use software to flag the fact that an individual was repeatedly buying stored value cards that are being used overseas, or that ATM withdrawals are repeatedly being made overseas. This itself raises a number of interesting points:

  - First, this would be a proprietary, commercial system. At this point, law enforcement agencies are not involved and we depend on the competence of the financial institution to detect suspicious activity.

  - Second, the obvious issue is where to set the threshold – i.e., at what point is activity deemed suspicious. It is crucial that the threshold be set at an appropriate point to avoid missing illegal activity or raising the alarm too frequently.

  - Third, it is important to bear in mind that financial institutions are primarily concerned with the detection of unauthorized transactions (for which they may be held responsible). Typically, the bank or credit card network will contact the account holder to find out if he or she authorized a suspicious transaction. If the account holder can verify the transaction, there is likely to be no further verification (until another threshold is crossed, presumably).
Which is the Greater Concern: Large-Value or Small-Value Transactions

The crucial question is (and this question is probably unanswerable): how long could a group of persons use the electronic payment systems in this way, and how much money could they launder, before being detected? The issue for regulators concerned with the prevention of money laundering and terrorist financing is: which is the greater risk – that a few large-value, illicit transactions will occur or that a series of many small-value, illicit transactions will occur? In this regard, the key aspect of the electronic payment systems is that while large-value transactions may be effected more quickly, they are also more likely to be detected. That being the case, is illicit use of electronic systems more likely to occur in the form of a series of smaller transactions which, while taking more time, would be less likely to be noticed?

Issues of Identity Verification

Considering the risk that electronic payment systems may be used to launder money also raises interesting questions about identity verification. First, it is important to note that identity verification serves different purposes in different contexts. For example, if an individual seeks to withdraw money from an account or to obtain credit, the financial institution is concerned with verifying that the person is who she says she is. Or, speaking more precisely, to verify that this individual is the same individual who controls the account or has a good credit record. On the other hand, if an individual seeks to open an account and deposit money, the bank has the opposite concern – that is, to establish that this individual is not one of the people listed on various watch-lists, with whom the bank is prohibited from doing business.

Upon reflection, it is clear that the second situation raises more difficult issues of identity verification, whether the transaction is electronic or effected in person. In the first case, the individual has the burden (and therefore has an interest in), proving that he or she is a particular person, in order to obtain the benefit of access to that persons
accounts. But in the second case, all the bank has is a name on a list, and perhaps a few other details. So we face the difficulty of a person who has access to more than one identity, as criminals often do. If a criminal presents herself to a bank, in person, with a passport or other identifying documents which match her own physical characteristics, the bank will have difficulty “proving the negative” – that is, establishing that the person does not have another identity which is an identity on a watch list – no matter how diligent the bank is.

Current security controls are more effective in preventing criminals from assuming the identity of some other legitimate person, in order to steal their money. That is, both the traditional, paper-based systems and the new electronic payment systems include means of preventing access to financial accounts by unauthorized persons. But in the second case – the money laundering and terrorist context – the person will assume a bogus identity and authorize transactions under that name, and the bank will never know that the person is actually someone who appears on a watch list.

For purposes of understanding the new electronic payment systems, the point is that they seem not to be any more vulnerable to the use of assumed identities for money laundering or other illegal activities than are the traditional systems. That is, it seems to be just as likely that bogus assumed identities could be used in the paper context as in the electronic context.

Last, just a few words on particular concerns that the threat of terrorism raises for electronic payment systems. First, it must be noted that the system itself can be a target of terrorist attacks, because it is a part of the critical information infrastructure upon which the international financial system depends. The vulnerability to such an attack arises primarily from the fact that the closed proprietary networks used by financial institutions have to be open to the Internet in order to conduct business. This provides an access point to terrorists. Since it is impossible to prevent terrorist attacks completely,
electronic payment systems must include measures to contain and remediate any security breaches.

**Balancing Difficulties Arising in Electronic Payment systems**

In conclusion, there are benefits and detriments in electronic payment systems in terms of the risk of money laundering and illegal activities. While it is true that electronic transactions can be effected more rapidly and from remote locations, it is also easier to maintain automatic records of such transactions or to put in place automated blockages of certain transactions. Similarly, while it is nearly impossible to verify the identity of someone who initiates a transaction remotely by electronic means, we must bear in mind that identity verification, in itself, raises a number of conceptual difficulties.
BACKGROUND

*1 In a complaint filed on October 5, 1996, the named plaintiffs “alleged that the defendants' practice of requiring merchants who accepted defendants' credit cards to also accept their debit products ... was an illegal tying arrangement, in violation of section 1 [of the Sherman Act].” In re Visa Check/MasterMoney Antitrust Litig., 297 F.Supp.2d 503, 507 (E.D.N.Y.2003). They “further alleged that, through these tying arrangements and other anticompetitive conduct, the defendants attempted to monopolize the debit card market, in violation of section 2 [of the Sherman Act].” Id. On February 22, 2000, this Court granted the motion to certify a class of “approximately four million merchants who have accepted Visa or MasterCard credit cards and who therefore have been required to accept VisaCheck and/or MasterMoney debit cards under the challenged tying arrangements during the fullest period permitted by the applicable statute of limitations”). The Second Circuit affirmed the class certification order on October 18, 2001. In re Visa Check/MasterMoney Antitrust Litig., 280 F.3d 124 (2d Cir.2001).

After motion practice, and just before opening statements were to begin at trial, the plaintiffs entered into preliminary settlement agreements with each of the defendants. Visa Check/MasterMoney, 297 F.Supp. at 508. These Settlement Agreements provided, among other things, for “the creation of a $3.05 billion settlement fund.” Id. On December 19, 2003, this Court issued an Opinion and Order approving the Settlement Agreements. Id. at 526, aff'd, 396 F.3d 96 (2d Cir.2005). The Amended Plan of Allocation provided that, “[w]hen distributions are otherwise complete, any monies remaining in the Net Settlement Fund ... will be applied in a manner recommended by Lead Counsel and approved by the Court.” (Amended Plan of Allocation § 12.7.)

On April 1, 2011, Constantine Cannon LLP (“Lead Counsel”) asked the Court to approve a plan requiring class members to cash their settlement checks by June 15, 2011 so that Lead Counsel could conclude the case. (ECF No. 1601.) Lead Counsel estimated that, after the deduction of expenses and in light of the anticipated check cashing, there would be approximately $1.7 million remaining in the fund —“only a miniscule percentage (0.7%) of the roughly $2.6 billion distributed to date.” (Id. at 4.) Consistent with the Amended Plan of Allocation, Lead Counsel proposed that “a cy pres donation of funds remaining in the settlement account” thereafter be made because “another distribution to the class would not be efficient or economically feasible.” (Id. at 1.) Lead Counsel accordingly requested that this Court order “that any residual funds left in the settlement account as of that date be donated to a charity or cause related to the merchant community to be approved by the Court.” (Id. at 4.) In support of its recommendation, Lead Counsel attached an affidavit of Neil Zola, President and Chief Operating Officer of The Garden
City Group, Inc. ("GCG"), the Claims Administrator retained by Lead Counsel. (Neil Zola Aff., ECF No. 1601–2.) Mr. Zola is also of the view that a further distribution to class members would not be economically feasible:

*2 Given the small percentage of remaining funds, GCG does not believe that any further Class distributions would be economically feasible because the cost to effectuate a distribution of the estimated available balance could exceed 50% of that balance. By way of example, if the more than 500,000 Class members who previously cashed their 2010 Distribution checks were eligible to receive another residual payment from the $1.7 million estimated remaining balance we would, at best, be able to distribute $900,000 since the rest would be used for the cost of printing 500,000 checks, postage for those checks, and handling all follow up, including thousands of check reissues. Moreover, if we distributed $900,000 to those eligible Class members, over 450,000 Class members would receive a check of less than $1.00. Further, another 42,000 Class members would receive a check in an amount between $1.00 and $5.00. In fact only 1.4% of Class members (about 7,100 merchants) would receive a check greater than $5.00. Therefore, GCG agrees with Lead Counsel that donating the balance of the remaining funds to charity is appropriate.

(Id. ¶ 15.)

By Order dated April 4, 2011, this Court set June 15, 2011, “as the final date by which all class members must cash their checks” and stated that “[a]ny residual funds left in the settlement account as of that date shall be donated to a charity to be approved by the Court.”

By letter dated June 15, 2011, Lead Counsel estimated that, given the number of checks that had been cashed, and in light of the anticipated deduction of costs and expenses, there would ultimately be “between $1.5 million and $1.6 million remaining in the settlement account available for a cy pres donation.” (ECF No. 1604.) “As such,” according to Lead Counsel, “at the end of the day, well over 99% of the funds that were available for distribution, net of expenses, were returned to the class”—resulting in a cy pres donation amount of “roughly 0.057% to 0.061% of the total amount distributed to class members.” (Id. at 1–2.) Lead Counsel asserted that this amount is “considerably lower than such distributions in similar cases.” (Id. at 2 & n. 1 (citing cases).)

In the same letter, Lead Counsel proposed that the settlement funds remaining after the final deadline for cashing settlement checks (net of remaining fees and disbursements) be given to the American Antitrust Institute ("AAI"), an organization that Lead Counsel's June 15, 2011 letter described as follows:

The mission of the AAI, a non-profit organization dedicated to education, research, and advocacy concerning antitrust law, is closely aligned with the substance and rationale of the case, as well as the interests of the class. The AAI has been the leading voice in urging more aggressive enforcement of antitrust laws—through private cases, such as In re Visa Check/MasterMoney Antitrust Litigation or via government enforcement—to increase competition in the interests of consumers and businesses such as the merchant class. See American Antitrust Institute, About Us, available at http:// www.antitrustinstitute.org/content/about-us, last visited June 12, 2011. In fact, through its advocacy the AAI attempts to create a substantive and procedural environment to enable more cases like In re Visa Check/MasterMoney
Antitrust Litigation, which will benefit businesses such as the merchant class and consumers alike. We can think of no better way to conclude this case than to make this contribution to this worthy cause. Cf. In re Publ'n Paper Antitrust Litig., 2009 WL 2351724, at *2 (D.Conn. July 30, 2009) (ordering that a cy pres award in an antitrust class action be distributed to the AAI, finding that “[b]ecause the plaintiffs’ claims here are based on antitrust injury, the next best use for the settlement funds is to disburse those funds to charitable institutions designed to guard against antitrust injury and protection consumers.”).

*3 (Id. at 3.)

By letter dated June 22, 2011, Consumers Union, a nonprofit advocacy organization and publisher of Consumer Reports, applied for an award of the cy pres funds. (ECF No. 1607.) The letter explained that the organization, which “does not accept advertising revenue or commercial donations,” does work “in the area of consumer financial protection,” an area that, according to Consumers Union, is “closely related both to the underlying subject matter of this antitrust action (payment card practices) and to an essential goal of antitrust enforcement: combating the impact that anti-competitive conduct has on consumers.” (Id. at 1.) The organization maintains that “[a] cy pres award could provide significant support as we expand our reach and impact to consumer constituencies that are particularly vulnerable to anti-competitive or predatory financial practices.” (Id.) With respect to its financial services policy and advocacy work, Consumers Union stated as follows:

While Consumers Union’s policy and advocacy work focuses on several pocketbook and safety issues, we have a particularly deep level of expertise and long commitment to helping consumers on financial matters. And we have a track record of success in this key area. For example, our financial services team works to help consumers make smart financial choices and avoid hidden fees on credit cards, debit cards, payroll cards, government-issued benefit cards, prepaid cards, mobile payments, checks and bank accounts. We seek to improve protections associated with existing payment methods, as well as emerging ones, through public education, consumer engagement, media outreach, policy reports, legislative and regulatory advocacy, social media outreach, and marketplace efforts.

Consumers Union was a leader in helping to shape and pass the landmark 2009 credit card reform law, as well as last year’s financial reform law establishing the Consumer Financial Protection Bureau. We are currently engaged in a Payments Project that focuses on newer ways to make payments that do not yet receive the same protections as credit cards. Our most recent research and policy white paper, entitled “Mobile Pay or Mobile Mess: Closing the Gap Between Mobile Payment Systems and Consumer Protections”... examines the complicated array of basic protections, and the troubling lack of protections on some of the newest products that consumers face while making purchases via their cell phones, and suggests ways to improve the marketplace.

The goal of this project is to understand existing and emerging payment methods facing consumers from various economic backgrounds, including lower-income consumers. We are evaluating the risks to consumers in new payment methods as they evolve, and working to improve products with substandard consumer protections before those methods spread widely. We reach out to media outlets and individual consumers to help us achieve marketplace change. A recent example is the Kardashian Kard, a debit card with particularly high fees, marketed to teenagers and young adults. Soon after the Kardashian Kard was launched, Consumers Union analyzed and reported on the card’s exorbitant fees; that work in part encouraged prompt removal of this high-priced product....

*4 We also continually bring to the attention of lawmakers, payment providers, the media and the public documented problems that consumers face when using existing payment methods. We do this through our Share Your Story database where we have collected thousands of personal financial experiences from individual consumers.
across the nation. (See www.defendyourdollars.org/share_your_story.html) These stories help us to develop a comprehensive understanding of the marketplace, inform consumers about emerging trends, fight for greater protections through marketplace engagement, and educate appropriate policymakers at the local, state and federal levels.

In addition, we have nearly one million consumer activists who receive our online information and who use our network to make their opinions on financial services issues known to lawmakers and regulators.

Finally, recognizing that Americans have the responsibility to change the way they handle credit, we have worked to educate the public on the best ways to avoid the pitfalls of debt through our online “Dangers of Debt” contest, social media, and educational campaign directed at young people and their parents.

(Id. at 2–3.) Consumers Union concluded as follows:

We believe that Consumers Union would make an excellent cy pres award recipient, offering an important means by which the Court can expand the benefits and impact of this historic antitrust settlement to consumers. It is, after all, consumers who bear the ultimate brunt of anti-competitive practices, either directly through means such as exorbitant or hidden fees, or indirectly via costs passed down in the form of higher prices for consumer goods.

(Id. at 3.)

In a letter dated July 5, 2011, Lead Counsel (which was in receipt of the letter from Consumers Union) stated that it was “sympathetic to the idea of distributing a portion of the funds to organizations dedicated to consumers—in fact, we view the American Antitrust Institute as just such an organization given the consumer welfare backdrop of antitrust law.” (ECF No. 1608.) It accordingly asked for three additional weeks to consider Consumers Union, as well as other consumer groups, as possible recipients of the cy pres donation. (Id.) This Court granted the request on July 7, 2011.

On July 27, 2011, Jewelers Vigilance Committee (“JVC”)—“a not for profit trade association dedicated to preserving the ethics and integrity of the U.S. precious metal, gem and jewelry trade to protect consumer confidence”—wrote to request consideration as a recipient of the cy pres funds. (ECF No. 1610, at 1.) In support of its application, JVC stated as follows:

Since 1917, the JVC has actively pursued education and outreach programs to foster and promote legal compliance with regulations and laws that govern our industry. We also actively work to protect consumers to ensure that their trust in our products (gold, silver, diamonds, color gemstones, etc.) is not violated. We have taken on the resolution of consumer complaints regarding trade practices, including advertising, product description, representations of quality, etc. Our work in the area of consumer protection is vital. Many consumer protection agencies (both not for profit and government agencies) refer such matters to us due to their lack of resources and expertise to take on these often complicated investigations and enforcement action. Without the JVC's activity in this area, there would be little, if any, action taken to represent and protect consumers of jewelry in the U.[.]S.

*5 The members of the JVC consist of all sectors of the jewelry trade—manufacturers, wholesalers, distributor [sic] and retailers, many of whom are also members of the class which is the subject of the above referenced litigation since they accept both MasterCard and Visa, as well as other credit cards and all forms of debit cards, for payment for these products at every level of the trade.... [W]e have the support of a wide array of jewelry companies for the consumer protection work that we do....
Since all of our members accept credit cards for payment, and because many of them fall victim to fraudulent practices associated with credit card use, JVC has undertaken an education program to help members of our trade to avoid losses due to credit card payments being reversed to their detriment. Our high value products are often targeted for purchase by money launderers, identity thieves or other criminals. The FTC recently issued regulations requiring businesses using credit cards to implement programs and policies to detect and prevent use of credit cards by identity thieves. In this regard, the JVC offers identification verification services which allow companies accepting credit cards to ensure that the card being proffered is not stolen and is in fact connected to the person offering it. We have also undertaken to educate our members about this law, as well as state and local requirements to protect the security of the data they gather from credit cards to ensure that data breaches do not occur and to mitigate any instances where identifying data has been made public.

Our budget for these kinds of (both consumer and trade protection) programs is quite small, and we are the only trade association doing the work. We are funded by member dues, and[,] as previously mentioned, our membership base is reducing in size due to the state of the economy. We can do more consumer outreach and trade counseling for members of the class if we have sufficient financial support to do so.

(Id. at 1–2).

By letter dated July 29, 2011, Lead Counsel supplemented its recommendation to the Court regarding the cy pres award. (ECF No. 1609.) Acknowledging that it has represented JVC in the past, Lead Counsel nevertheless “respectfully recommend[ed] that the Court deny [JVC’s] request to participate in the distribution,” because “the JVC members that were members of the class have already benefitted from the settlement and the distribution” and because Lead Counsel is “disinclined to endorse such a narrowly tailored interest[’s] receiving a portion of the funds, particularly when its connection to the underlying case and the issues it concerned is so attenuated.” (Id. at 3.) Lead Counsel instead reiterated its recommendation that the entire cy pres distribution be granted to AAI, but further stated that “to the extent the Court would like to include consumer organizations in the distribution we respectfully recommend that 2/3 of the award be given to the AAI, with the remaining 1/3 awarded to one or two worthy consumer organizations.” (Id. at 2.) While “laud[ing] the work that Consumers Union does on behalf of consumers,” Lead Counsel expressed the view that U.S. PIRG “would be an equally worthy recipient of the funds that the Court decides to allocate to consumer groups,” (id. at 2–3), saying:

*6 PIRG is a network of state public interest groups working on behalf of the American public on issues such as product safety, public health and health care reform, higher education, political corruption and voting rights. See http://www.uspirg.org/about-us. PIRG has also been among the most active consumer groups on issues pertaining to the high, and hidden, costs of payment cards to consumers. PIRG, for example, submitted comments to the Federal Reserve with respect to its recent rulemakings on debit interchange that were indicative of the sophisticated approach it brings to bear on these issues ... Accordingly, to the extent the Court chooses to include consumer organizations in the cy pres distribution, we respectfully recommend that 1/3 of the available funds be given to PIRG or split between PIRG and Consumers Union.
Lead Counsel's July 29, 2011 letter also provided the following additional information about AAI:

As noted earlier, the AAI is a non-profit organization dedicated to education, research and advocacy concerning antitrust law. It was the first public interest group to focus on promoting more aggressive antitrust policies and enforcement to maintain competition and protect consumers and small businesses. On virtually all complex antitrust issues, the AAI offers a unique voice in favor of vigorous private and public enforcement of the antitrust laws. It has advocated on behalf of consumers and small businesses in Congress, before agencies and courts, on the state level and internationally on a wide range of issues, from health care and pharmacology to retailer concerns. In that capacity the AAI conducts industry studies and joint programs with foreign antitrust enforcers, submits testimony and comments on agency policies and enforcement practices and files amicus briefs on important antitrust issues before the Supreme Court and the Appellate Courts. For example, in the past decade it has filed roughly 50 amicus briefs, including in American Needle, Inc. v. National Football League, — U.S. ——, 130 S.Ct. 2201, 176 L.Ed.2d 947 (2010), in which the Supreme Court adopted the AAI's argument. In Pacific Bell Telephone Co. v. Linkline Communications, Inc., 555 U.S. 438, 129 S.Ct. 1109, 172 L.Ed.2d 836 (2009), the Supreme Court invited the AAI to provide a 15–minute oral argument, believed to be a first for a non-governmental third party in an antitrust case....

Notably, the AAI's advocacy efforts have included a long-standing interest in the interchange issues central to In re Visa Check/MasterMoney Antitrust Litigation. It issued a report over a year ago calling for a policy change that would have Congress giving the Federal Reserve power to mandate lower interchange fees. After the Durbin Amendment granting such power was passed, the AAI continued the fight in the face of heavy opposition to implementation of the amendment, submitting a letter to Congress urging support of the new policy. *7 Like its advocacy efforts, the AAI's efforts to educate the public about the importance of antitrust are also wide-spread and effective. These efforts include publishing over 100 articles and reports on pressing antitrust issues, producing an award-winning documentary on U.S. antitrust law that was shown on public television and developing an accompanying educational curriculum for high school classrooms (see www.fairfightfilm.org) and hosting several conferences and symposiums on antitrust issues. The AAI's website, which offers a vast array of resources to the public, including resources aimed specifically at aiding consumers, has been called “the best one-stop antitrust site out there” by Legal Times. The AAI has also contributed to antitrust scholarship in other ways. For example, in 2010, it published its third book, The International Handbook on Private Enforcement of Competition Law. It is currently preparing a book on private enforcement in the U.S. Under another cy pres grant, the AAI is also currently preparing a curriculum for the training of judges.

The AAI is still a young organization, nearly fifteen years old. Its highly qualified five-person staff works from private homes around the U.S. AAI is about to enter the always-difficult transition to a second generation of leadership as its president and some board members approach retirement in the next two years. The AAI depends on cy pres grants and other unpredictable contributions, making long-term planning and long-term employment commitments particularly difficult. A full distribution to the AAI at this time would provide much of the financial base that will allow it to recruit the next generation of leadership and retain its excellent staff thereby guaranteeing the nation the continuing public interest services it provides. In sum, it is our hope that providing the full distribution to this worthy organization will endow it well into the future and we fear that, given the amount of the distribution, balkanizing the award between the AAI and other recipients
will undermine that objective. For these reasons, we repeat our initial recommendation to the Court.

(Id. at 1–2 (exhibit citations omitted; italics added).)

By a letter also dated July 29, 2011, Consumers Union supplemented its prior application by providing the Court with a copy of an article to appear in the September 2011 edition of Consumer Reports, entitled “New ways to pay: At the checkout, should you use credit, debit or cell phone?” (ECF No. 1611.) Consumers Union's letter highlighted the following excerpts from the article:

Most of the new electronic payment options are tied to credit and debit cards, so whatever costs you incur in using your plastic will transfer to the new methods. But some costs are completely hidden, so consumers are often unaware of the price of their payment-choice decisions....

For example, banks have long charged a fee of 1 to 4 percent of the purchase amount, depending on whether debit or credit was used. That fee is levied on retailers, so consumers don't see it up front, but they pay it in higher merchandise prices. “The average household pays $427 a year in transaction fees to card companies and banks that they don't know they're paying....”

*8 (Id. at 2.) The article advises consumers to “never pay a fee to pay by debit” and asserts that “[s]uch fees ... aren't common, but some merchants impose them. Refuse, cancel the sale, and report the merchant to your debit-card issuer.” (Id. at 2 (quoting article).) Consumers Union asserts that the article offers “a good example of our ongoing journalism, education and advocacy efforts on hidden costs.” (Id.) The letter concludes:

A cy pres award from this settlement would be timely indeed, potentially providing significant funding for our efforts to inform, protect, connect and empower consumers in the area of personal finance and payment card fees. It would, for example, assist us in expanding our reach to minority and younger consumer communities, such as those going off to college, using creative methods such as animated videos, contests and school/campus programs.

(Id. at 3.)

In a letter dated August 5, 2011, Lead Counsel informed the Court that Jeffrey Shinder and Doug Rosenthal of Constantine Cannon LLP (Lead Counsel), and George Sampson of Hagens Berman (a firm that also represents the class), are members of the AAI advisory board, and that Lloyd Constantine, also of Constantine Cannon LLP, is a former member of the advisory board. (ECF No. 1612.) Lead Counsel explained that advisory board members “receive no compensation or other potential benefit from their roles as advisory board members” and that they “recuse themselves ... when conflicts of interest arise due to conflicting client matters or past governmental roles.” (Id. at 1.) Lead Counsel noted that AAI's website lists its advisory board members. (Id. (citing http://www.antitrustinstitute.org/content/people).)

On September 14, 2011, after ordering the payment of various fees and expenses from the remaining funds, the Court directed Lead Counsel to remit what remained of the settlement fund to the Clerk of the Court on or before September 16, 2011. (See also Sept. 15, 2011 Order, ECF No. 1620 (directing Clerk of the Court to place remitted funds into an interest-bearing account).) On September 16, 2011, Lead Counsel sent the Clerk of the Court two checks in the amounts of $1,750,473.29 and $22,734.79. (ECF Nos. 1621, 1622.) On October 18, 2011, Special Master Robin Wilcox submitted her final bill in the amount of $24,702.15.
This Court has "broad supervisory powers with respect to the administration and allocation of settlement funds." In re Holocaust Victim Assets Litig., 424 F.3d 132, 146 (2d Cir.2005) (internal quotation marks omitted); see also id. at 147 (noting that, in In re Airline Ticket Commission Antitrust Litigation, 268 F.3d 619, 626 (8th Cir.2001), the Eighth Circuit concluded that a cy pres allocation is within the Court's discretion unless the Court "(1) fails to offer any indication of having carefully weighed all of the considerations relevant to the allocation; and (2) makes no findings in connection with its distribution of funds"). "A cy pres payment, as an adjunct to a payment by other means to some members of the class, is warranted where the amount to be distributed to the remaining class members is small relative to the administrative costs of a direct distribution." In re MetLife Demutualization Litig., 689 F.Supp.2d 297, 343 (E.D.N.Y.2010).

An additional distribution in this case would involve prohibitively high administrative costs. Checks that would be sent to class members in connection with such a distribution would be de minimis. Therefore, it is clear to me, and I hereby find, that a cy pres award is a more appropriate manner by which to dispose of the remaining settlement funds than would be an additional distribution. The question, then, is to which charitable organization or organizations this award should be made.

Each of the organizations that has applied for or has been mentioned as a potential recipient of an award from the remaining funds is a worthy cause. However, "the purpose of Cy Pres distribution is to put the unclaimed fund to its next best compensation use, e.g., for the aggregate, indirect, prospective benefit of the class." Masters v. Wilhelmina Model Agency, Inc., 473 F.3d 423, 436 (2d Cir.2007) (internal quotation marks and alterations omitted); see also id. ("Cy Pres means 'as near as possible'....."). Based on this standard, I agree with Lead Counsel that JVC is not an appropriate recipient. The JVC members who were members of the class have already benefited from the settlement and distribution. I am, moreover, concerned that an award to a cause with such narrowly tailored interests would have the effect of inequitably concentrating its benefit on a subset of the class as opposed to the class as a whole.

Bearing in mind the interests of the entire class and all of its members, I believe that the award should be spread among the three remaining charities described above—AAI, Consumers Union and U.S. PIRG. AAI has made significant contributions to the development and enforcement of the antitrust laws and will no doubt make effective use of the funds it receives. Similarly, both Consumers Union and U.S. PIRG have devoted substantial resources to issues that are closely related to the interests of the members of this class—including, for example, issues pertaining to the high and hidden costs of payment cards.

To account for the fact that each of these organizations does work that benefits the class in different ways, I hereby order the distribution of the amount remaining after the payment of the Special Master's final bill as follows: 50% to AAI; 25% to Consumers Union; and 25% to U.S. PIRG.

CONCLUSION

For the reasons described above, I hereby direct the Clerk of the Court to make payment to the Special Master in the amount of $24,702.15. I further direct that the remaining funds be distributed as follows: 50% of the amount that remains after the payment of the Special Master's bill to the American Antitrust Institute, 25% to Consumers Union and 25% to U.S. PIRG.

So ordered.

Parallel Citations

2011-2 Trade Cases P 77,654
CONFUSION AND CONVERGENCE IN CONSUMER PAYMENTS: IS COHERENCE IN ERROR RESOLUTION APPROPRIATE?

ANITA RAMASASTRY*

INTRODUCTION

When Joe Consumer reaches the checkout at the grocery store, he has multiple ways to pay for his groceries. He can write a check and hand it to the cashier. This check, however, might get converted into an Automated Clearinghouse (ACH) transaction, which results in a funds transfer from his bank account. He might also use several different types of plastic to pay for his groceries—including a debit card, a credit card, or a prepaid gift card, perhaps issued by his own supermarket chain. For Joe Consumer, the methods of payment may appear quite similar in terms of how they are used and electronically processed, but the legal rules which govern each transaction vary. Joe Consumer might also pay for his groceries by shopping online. Perhaps he will pay his online grocery bill using his PayPal account. The rules which govern these transactions will also vary.

Does Joe Consumer know which rules govern each transaction? While there is no empirical research about this, it is hard to imagine that most consumers are aware of the differing rules that stem from each payment.1

In the United States, Congress and federal regulators have attempted to foster innovation in the payments arena by regulating new payment methods after they have gained consumer acceptance.2 Regulators often try to craft regulatory responses that are not burdensome to industry and are

---

* Associate Professor of Law and Director, Shidler Center for Law, Commerce & Technology, University of Washington School of Law. The author would like to thank the organizers of the symposium and payments conference, and in particular Professor Steven Harris, Professor Linda Rusch, and Stephanie Heller for the opportunity to participate in this important event.

1. When the author teaches payment systems at her law school, she surveys her students to find out how much they know about error and fraud rules with respect to different consumer payment methods. Students typically are unaware of the varying rules and where they come from. Few students have read their deposit, debit, or credit card agreements.

tailored to the specific aspects of particular payment systems. This has led to a consumer payments regime with different rules for different systems. To date, legislators and regulators have failed to enact a uniform approach to consumer payments.3

There are at least three distinct primary consumer payments regimes—credit cards, debit cards/electronic funds transfers, and checks—and they are each governed by differing regulatory regimes. As a result, their error resolution mechanisms, among other things, vary.4 At present, error resolution for checks is governed by Article 4 of the Uniform Commercial Code. If a consumer discovers an error with respect to a check, the bank’s duty to rectify the error comes from U.C.C. section 4-401. A bank must only pay checks that are properly payable and bears responsibility for checks that are wrongfully honored. There is, however, no formal timeframe within which a bank must act. A consumer, on the other hand, must notify the bank with reasonable promptness about certain types of errors (which can be detected by reviewing her bank statement).5 This time limit can be specified by the terms of the account agreement between a consumer and his financial institution. Some banks give consumers one to two weeks to report errors, for example.


4. For checks, Articles 3, 4, and 4A of the U.C.C. govern check transactions. U.C.C. art. 3 (2005) (Negotiable Instruments); U.C.C. art. 4 (2005) (Bank Deposits and Collections); U.C.C. art. 4A (2005) (Funds Transfers). In terms of error resolution, U.C.C. section 4-401 sets forth a rule that a bank may only pay a check that is properly payable. To the extent that a check is paid which contains an alteration or forgery, the drawer has real defenses available as a grounds for non payment because it is not properly payable. See U.C.C. § 4-401 cmt. 1. Regulation E outlines detailed procedures that financial institutions must use for error resolution, including: informing consumers of the availability of error-resolution services, procedures, and timetables for investigating errors; the extent of the required investigation; and procedures that must be followed after the investigation is completed. For example, if the institution has not completed its investigation of an ACH E-Check transaction within ten days, it must provisionally recredit the consumer’s account in the amount of the potential error and complete the investigation within forty-five days. Furletti, supra note 2, at 20; Mark Furletti & Stephen Smith, The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: Credit and Debit Cards 23–24 (Fed. Reserve Bank of Phila., Discussion Paper No. 05-01, 2005), available at http://www.philadelphiaged.org/pcc/papers/2005/ConsumerProtectionPaper_CreditDebitCard.pdf.

5. U.C.C. § 4-406.
Error resolution for funds transfers such as debit card transactions are governed by Federal Reserve Regulation E and the Electronic Fund Transfer Act (EFTA). Regulation E sets out a more detailed error resolution procedure. A consumer has sixty days after the transmission of a bank statement to alert a financial institution of an error. After that the institution has to act within a set timeframe, and if it cannot resolve an error within ten business days, it must provide a consumer with a provisional recredit. A bank must also complete its investigation within forty-five days.

Credit card error resolution is governed by Federal Reserve Regulation Z. The billing error resolution procedures for credit cards are quite similar to those for debit cards and funds transfers. In contrast, stored-value and prepaid cards offer no statutory error resolution procedures with the exception of certain types of payroll cards.

Some commentators have suggested that there is a great deal of consumer confusion surrounding new electronic payment methods. There has been, however, little research into consumer understanding of consumer protection laws as they apply to different payment methods or into whether differing regulation impacts consumer choice. At the same time, some preliminary facts suggest that consumers may indeed be confused by the patchwork of payment regulations governing the ways in which they pay and transact. At times, it is unclear whether consumers understand the differences in their legal or statutory rights arising from use of different payment methods. Scholars have also questioned the basis for maintaining the distinctions in legal rules for different payment systems.


8. The STAR Consumer Payments Usage Study, conducted by First Data Corporation, found that consumers use between two and four different payment types each month. As part of the study, consumers were asked about identity theft and fraud protections:

  Overall, less than one-fifth of debit card users surveyed are aware of zero liability from any type of debit card losses. However, when asked about personal liability and exposure to fraudulent purchases, consumers were equally likely to expect zero liability from signature debit and PIN-secured debit purchases. Financial institutions have an opportunity to better educate their cardholders about the protective features of their cards.

This lack of uniformity has been heightened by the growth of new payment mechanisms. Some of these mechanisms, operated by non-banks, piggyback off of existing payment mechanisms such as bank accounts and credit cards. The providers of these mechanisms add another payments layer to transactions. These new payment mechanisms or systems are referred to as payment “intermediaries.” Non-bank intermediaries serve as conduits to allow payments from one person or entity to another with the initial source of funds being paid into a new account maintained by the intermediary. The funds may be transferred into the new account through a choice of payment methods.

In recent years, there has been a lack of certainty among regulators and market participants as to when such intermediaries are regulated and under what type of regulation for different points of a consumer transaction. Since they offer payment choice, the funding stream for each transaction may determine what rules apply. This may not, however, be readily apparent to the consumer.

Furthermore, new variations on existing payment methods have caused payment methods to change midstream. Electronic check conversion, for example, can transform a paper check into an electronic funds transfer governed by the EFTA and Regulation E. Consumers may not be aware that payment methods can and may be transformed through use of an intermediary or through conversion of a payment instrument into a funds transfer.

The growth of prepaid cards and stored value is another significant factor which may have led to consumer confusion. As consumers use prepaid cards in a manner that replicates the use of a debit card, for example, at a point-of-sale (POS) terminal, they may expect that such card is treated


10. In 2005, the Federal Reserve Board proposed amendments to Regulation E to cover merchants with respect to electronic check transactions. Consumers must now receive notice if their checks will be processed electronically either at the point of sale or when they are remitting payments as part of a lockbox or accounts-receivable transaction. The impetus for such notice relates to consumer confusion. Today, when a consumer mails a check for payment to a credit card issuer, the transaction may be covered by three separate sets of rules. Consumer confusion may be further exacerbated because the consumer will not know at the time he mails the check which method of processing will be chosen by the credit card biller. See 12 C.F.R. § 205.3 (2007); see also Mark E. Budnitz, Consumer Payment Products and Systems: The Need for Uniformity and the Risk of Political Defeat, 24 ANN. REV. BANKING & FIN. L. 247, 255 (2005).
the same as a debit card. The term "prepaid" debit card is emblematic of this phenomenon. In fact, however, most such cards, even when carrying large balances, are not regulated by the Federal Reserve.

When consumers have competing methods from which to choose, does the lack of uniformity impact their choice of payment method? Is a lack of uniformity leading to less efficiency and predictability in the changing retail payments market? In the absence of regulation, will unregulated entities invest in appropriate error resolution mechanisms? Does consumer confusion lead to market failure with respect to efficient types of error resolution in retail payments schemes?

This article examines apparent sources of consumer confusion with respect to different retail payment methods and the consumer protections which may or may not flow from each method. The article examines how consumer confusion appears to be exacerbated or impacted because payment methods, which were previously distinct, are now routinely woven together, either through the emergence of new payment vehicles or through changes in electronic payment processing. This blending and convergence may cause consumers to have unclear expectations as to what rules govern their transactions at a given point in time.

As payment methods converge, the electronic funds transfer is becoming a central payment mechanism for the consumer (whether or not such a transfer is regulated under the Electronic Fund Transfer Act or Federal Reserve Regulation E). Given existing confusion and the related convergence, is it time to revisit the need for uniformity in consumer payment rules? This article examines one aspect of uniformity: error resolution.

Part I of this article examines the situations where consumer confusion may exist with respect to different payment methods, including an examination of the role of payment intermediaries, the growth of electronic check conversion, and the increasing consumer use of prepaid cards. Part II of

11. The U.S. Department of Justice defines stored-value cards as follows:
Open system cards operate on major credit card networks and can be used anywhere that the network brand is accepted, frequently including worldwide ATMs. These cards are similar in appearance to traditional debit cards and are embossed with the cardholder’s name. Semi-open system cards generally have the same features and limitations as open system cards but cannot be used to access cash at ATMs.


this article asks whether uniform rules governing error resolution might be desirable given the confusion and incoherence which currently exists. This article suggests that there is a market failure when it comes to error resolution in payments.

The goal of such a change would be to provide greater certainty and predictability with respect to error resolution for a broader range of consumer payment vehicles. With certainty and predictability, consumers may be more confident in adopting newer payment methods, and will do so without confusion as to which rules may govern the various aspects of their transactions. As for loss allocation, a change in rules would allow payments providers to operate with clear and consistent rules for all types of transactions. It would also create incentives for financial institutions and payments processors to invest in technology to reduce and detect processing errors. Moreover, merchants and consumers alike would have the benefit of the same type of procedures for payment related errors—irrespective of which method a consumer chooses to use to transact.

Would it be desirable to have more uniform rules with respect to error resolution for a larger class of consumer payment mechanisms? Consumers may already be getting such benefits with respect to checks, because of electronic check conversion. As more payments converge and become funds transfers, is it time to unify error resolution mechanisms? The article makes a proposal: Regulation E-style error resolution should be made clearly applicable to payment intermediaries and possibly to other payment mechanisms, with a more limited application of the periodic statement requirement found in Regulation E.

This article argues that, at a minimum, it is time to extend Regulation E and the EFTA to clearly encompass payment intermediaries as a means of foreclosing existing ambiguities or gaps in regulatory coverage. It also explores the theoretical basis for uniform error resolution mechanisms, and contemplates the expansion of Regulation E to a larger class of stored-value and prepaid card products. The extension of Regulation E could either replicate the manner in which payroll cards were incorporated into the regulation or use a time period linked to the date of the transaction rather than a periodic statement. Rather than having to provide each customer with costly printed periodic statements, general purpose stored-value issuers or payment intermediaries could focus on providing transaction histories in electronic form or over the telephone. At the same time, a consumer could obtain a written transaction history solely upon request.
Finally, this article concludes that in the absence of federal regulation, the use of state licensing laws (such as money transmission laws) can be used to ensure that payment system providers that remain unregulated at the federal level or where regulation is not clear still provide consumers with adequate means of redress and error resolution. The ability of a state regulator to impose requirements as part of a safety and soundness regime, or as part of licensing requirements, may be a useful alternative as the Federal Reserve Board continues to examine the role of intermediaries and prepaid card issuers.

This article focuses on the procedural issues surrounding error resolution. It uses this as a means of exploring the desirability (or lack thereof) of uniformity in procedure. It does not delve into the issues of liability limitations or the ability of a consumer to use the payment system to challenge a merchant with respect to an underlying contract. Rather, this article focuses on error resolution and the processes by which a consumer has a right to have his account recredited and an investigation commenced with respect to processing errors which occur when he makes a payment using a mechanism such as a check, credit card, or debit card.

For the purposes of this article, the term “error resolution” has been borrowed from the Electronic Fund Transfer Act and Federal Reserve Regulation E to include, inter alia, the following types of errors:

(i) An unauthorized electronic fund transfer [to the extent it needs to be reported as part of an error resolution process];
(ii) An incorrect electronic fund transfer to or from the consumer’s account;
(iii) The omission of an electronic fund transfer from a periodic statement;
(iv) A computational or bookkeeping error made by the financial institution relating to an electronic fund transfer; [and]
(v) The consumer’s receipt of an incorrect amount of money from an electronic terminal.

---

13. This issue has been addressed in other articles. See, e.g., Clayton P. Gillette, Rules, Standards, and Precautions in Payment Systems, 82 VA. L. REV. 181 (1996) (evaluating the differing liability regimes for credit cards and checks with respect to unauthorized use); Mann, supra note 3 (evaluating the credit/debit distinction with respect to differing liability rules for credit and debit cards).

14. 12 C.F.R. § 205.11(a)(1) (2007). Under Truth in Lending (Regulation Z), 12 C.F.R. § 226.13(a), the definition of a billing error is as follows:

(1) A reflection on or with a periodic statement of an extension of credit that is not made to the consumer or to a person who has actual, implied, or apparent authority to use the consumer’s credit card or open-end credit plan.

(2) A reflection on or with a periodic statement of an extension of credit that is not identified in accordance with the requirements of §§ 226.7(b) and 226.8.
I. THREE SCENARIOS THAT MAY CAUSE CONFUSION WITH RESPECT TO ERROR RESOLUTION IN CONSUMER PAYMENTS

What is the current status of error resolution with respect to emerging electronic payment methods? There are at least three types of emerging payment methods where the status of error resolution is unclear or where payments may be unregulated with respect to consumer error resolution. The legal framework for consumer error resolution has not been updated sufficiently to clearly encompass new types of transactions.

Part I of this article discusses how various error resolution rules apply to new electronic payment methods and highlights the ambiguities or gaps in the current regulations.

Some of the events that have given rise to potential consumer confusion include (i) the emergence of payment intermediaries that facilitate payments using multiple methods, (ii) the growing use of electronic check conversion, which transforms a negotiable instrument into an electronic funds transfer, and (iii) the emergence of prepaid cards as an important payment substitute that has the characteristics of an electronic funds transfer but is typically not treated as one for regulatory purposes.

A. Scenario One: Payment Intermediaries

1. P2P Payments

Person-to-Person or Peer-to-Peer (P2P) payments providers are those who allow their customers to open accounts and to move money between those accounts. PayPal is a large and successful example of a P2P payment provider.15 P2P payments providers have also been referred to as Internet funds transfer providers. Such services allow consumers to move money

---

(3) A reflection on or with a periodic statement of an extension of credit for property or services not accepted by the consumer or the consumer's designee, or not delivered to the consumer or the consumer's designee as agreed.

(4) A reflection on a periodic statement of the creditor's failure to credit properly a payment or other credit issued to the consumer's account.

(5) A reflection on a periodic statement of a computational or similar error of an accounting nature that is made by the creditor.

(6) A reflection on a periodic statement of an extension of credit for which the consumer requests additional clarification, including documentary evidence.

(7) The creditor's failure to mail or deliver a periodic statement to the consumer's last known address if that address was received by the creditor, in writing, at least 20 days before the end of the billing cycle for which the statement was required.

over the Internet or through another device, such as a PDA or a cell phone, to another consumer or merchant. P2P payments providers, such as PayPal, allow consumers to open online accounts with a provider directly. These are referred to as "accounts" but are not individual depository accounts which are held by banks.16

a. **Funding a P2P Account**17

There are multiple ways in which a person who wishes to use a P2P payments service can "prefund" a P2P account. First, a customer could fund an account using an ACH bank transfer. Second, a customer could fund his account using a credit card or a debit card. A third choice would be funding the account using prepayment, such as by sending in a check or money order.18

b. **Transferring Funds/Making Payment**19

When a user (for example, an auction buyer) wishes to send money to another person (for example, an online auction seller) in the P2P environment, a user may have several choices. Funds may be sent from a user's account with the P2P provider. For example, a PayPal customer can send funds that are parked in his PayPal account to another PayPal account holder.20 Alternatively, the same user could request that payment be made directly from his bank account. The P2P intermediary would facilitate the transfer, assuming the user had given the intermediary authority or information to debit his bank account. A user could alternatively charge his credit card directly or provide a debit card number in order to make payment. In each case, an intermediary is the entity that facilitates the transaction.

What happens if there is an error in the payment made, such as a duplicate payment or a payment in an incorrect amount? The answer to this question should mirror the type of payment mechanism used to either fund a P2P account or to make payments on behalf of a P2P customer.

18. See PayPal, supra note 16, § 3.2-3.3.
19. Ramasastry, supra note 17, at 670-71; Mann, supra note 17, at 684-86.
If an account is funded with a credit card, the protections of the Truth in Lending Act (TILA) and Regulation Z should apply. By contrast, if an account is funded by bank transfer, this would trigger the EFTA and Regulation E.21 If a consumer prefunded a P2P account by check, Articles 3 and 4 of the U.C.C. would apply to the transaction.

What about erroneous payments made via a P2P intermediary? First, one might state that if the payment were made with a credit card, TILA and Regulation Z should apply. This would be important to the extent that a user has a dispute with a merchant to whom he had sent funds. For example, a consumer that received defective goods from a PayPal seller, and who made payment using a credit card, might expect that she could use the chargeback provisions under Regulation Z in the event that there was a problem with the contract, or use the “billing error” provisions of Regulation Z if the goods were not delivered at all. At least one credit card issuer, however, previously asserted that it was making a payment of funds rather than facilitating an underlying transaction—akin to a cash advance. Under that scenario, Regulation Z’s chargeback provisions would not apply.22 For consumers, the choice of funding method would lead to different consumer protections—even though the intermediary (PayPal) would be the same in each case.23

As an alternative, a PayPal buyer might make payment directly from his PayPal account (user account) or via a bank transfer. In the case of a bank transfer, Regulation E would apply. But what about situations where a consumer uses her P2P account to make payment to someone? In those situations, the applicable rules were initially not apparent to regulators and

21. Mann, supra note 3, at 634, 649. Ronald Mann comments: [I]f the buyer has the good luck (or foresight) to fund the purchase directly from a credit card, the transaction is governed by the TILA/Z regime. Thus, among other things, the purchaser should have the right to withhold payment if the seller in fact never supplies the goods. The statute grants a broad right to the cardholder to withhold payment based on “all claims (other than tort claims) and defenses arising out of any transaction in which the credit card is used as a method of payment.” Thus, if the transaction through PayPal is viewed as a single unified transaction in which the auction purchaser uses PayPal and the credit card to buy something from an auction seller, the TILA/Z regime protects the purchaser.

Mann, supra note 17, at 696 (quoting 15 U.S.C. § 1666i (2000)).

22. As Mann notes:

The statute could be read more narrowly. American Express, for example, apparently has argued that the transaction is one in which PayPal is the seller and that PayPal has satisfied its obligation by sending money to the seller. On that understanding, American Express (or any other card issuer with the boldness to raise the argument) would have no obligation to respect the defense under 15 U.S.C. § 1666i. Even American Express, however, receded from that position after it was challenged recently by the New York Attorney General.

Id. at 696 n.87.

23. Id. at 695–96.
COHERENCE IN ERROR RESOLUTION

consumers. Some commentators noted that it was unclear what law would apply to a funds transfer made directly from a P2P user's account to another user's account. In other words, would such a transfer from a non-bank account constitute a "funds transfer" under Regulation E? Ronald Mann has pointed out that such a transfer is covered by Regulation E and that a PayPal account would qualify as an account under Regulation E. While Mann is correct, this point was not initially clear to consumers and other stakeholders.

Recent litigation against PayPal further highlights the uncertainty that arose with respect to the role of P2P providers in the payments chain. In 2002, PayPal was the subject of multiple class action lawsuits, which focused on the company's obligations pursuant to the EFTA. The lawsuits were consolidated into one lawsuit in the United States District Court for the Northern District of California, San Jose Division.

The consolidated lawsuit alleged that PayPal had violated the EFTA by failing (i) to provide its customers with information about its dispute resolution procedures, and (ii) to follow certain procedures when handling complaints of unauthorized or erroneous funds transfers. For example, the lawsuit alleged that PayPal did not provide account statements in the man-

25. Mann, supra note 17, at 695–96.
26. Settlement Agreement at 1–2, In re PayPal Litigation, No. CV-02-01227-JF/PVT (N.D. Cal. June 11, 2004). According to a settlement document that seems to have been sent to potential class members:

In early 2002, Plaintiffs Roberta Toher and Jeffrey Resnick filed separate lawsuits against PayPal, Inc. These two cases were later consolidated into one lawsuit in the United States District Court for the Northern District of California, San Jose Division, entitled In re PayPal Litigation, Case No. CV 02 01227-JF (PVT). The lawsuit alleges that PayPal violated the federal Electronic Fund Transfer Act . . . including provisions requiring PayPal to supply customers with information about dispute resolution procedures and to follow certain procedures when investigating complaints of unauthorized or incorrect electronic fund transfers. For example, the lawsuit claims that PayPal did not provide account statements in the manner required by the EFTA. The lawsuit further alleges that PayPal has placed inappropriate restrictions or other limits on customers' accounts and engaged in other improper practices. Based on these practices, the lawsuit asserts claims under California state law for conversion; money had and received, negligence, and violations of consumer protection statutes.

PayPal does not believe that it did anything wrong. In fact, PayPal disputes that the EFTA, originally passed in 1978, applies to its business. PayPal denies any and all liability for the claims alleged in the lawsuit. The Court did not decide in favor of the Plaintiffs or PayPal. Instead, beginning in the fall of 2003, the parties began a series of settlement negotiations mediated by United States Magistrate Judge Edward Infante. Eventually, in November 2003, both sides agreed to a settlement in principle. By settling their claims, both parties avoided the uncertainty and cost of a trial. The settlement provides money and other benefits to the Class. On June 11, 2004, the parties entered into a formal, written Settlement Agreement . . .

The lawsuit further alleged that PayPal had incorrectly removed funds from consumer accounts and made erroneous charges to those accounts as well. 28

During the fall of 2003, the parties began a series of settlement negotiation sessions mediated by the court. 29 On June 11, 2004, the parties entered into a formal settlement agreement. 30 The settlement requires that PayPal consent to the entry of a court-ordered injunction that mandates various changes to its business practices. At the time of settlement, PayPal stated that it had already implemented these changes. The injunction included PayPal's agreement to comply with certain notice and error resolution procedures of the EFTA, and to follow certain procedures for limiting accounts and responding to and returning funds to customers whose accounts had been restricted. 31 When PayPal settled, it did not admit it was subject to the EFTA. Instead, the company established a settlement fund to provide compensation to consumers who had previously sought remedies under the EFTA. 32

More recently, during the fall of 2006, twenty-eight states' attorneys general reached a settlement with PayPal that also related to consumer confusion as to applicable rights and governing consumer protection rules for PayPal transactions. The settlement document states that “[t]he parties agree that different terms of the consumer protection programs, their relationship to credit card and chargeback rights, and the pre-existing differences between the EFTA and FCBA [the Fair Credit Billing Act] may have caused some confusion among Users making Payments.” 33

As part of the settlement, PayPal has agreed to “summarize on the funding source information Webpage the different statutory rights and remedies available for Payments under the EFTA and FCBA to Users for the different types of funding sources that may be used to fund Payments.” 34 The settlement notes that “PayPal will also provide . . . a Clear and Conspicuous statement which advises that the User should, prior to

28. Id. at 5, 8–11.
30. Id. at 1.
31. Id. at 3.
32. Id. at 8.
34. Id. ¶ 12(f(ii).
committing to the addition of a bank account, review and understand the rights and remedies available for different Payment sources under the EFTA and FCBA.\textsuperscript{35}

The settlement also notes that unless PayPal is operating as a credit card issuer, it will not advertise "that its Payments services give consumers the rights and privileges expected of a credit card transaction."\textsuperscript{36} Rather, PayPal may state that Users who fund payments using a credit card will be eligible for the same protections from their card issuer as if the user’s credit card had been given directly to the merchant. PayPal also agreed to the following:

PayPal will not in its User Agreement or seller and buyer protection programs use branding, descriptions or representations (including but not limited to use of the terms "electronic funds transfer," "error resolution," "unauthorized transaction," "billing error," and "chargeback") in a way that is likely to cause confusion by leading Users to believe that by using the PayPal programs they are exercising rights pursuant to state or federally mandated consumer protection laws or rules that do not apply to such programs.\textsuperscript{37}

One would assume that, for transfers that are made from a customer’s bank account as payment, this would constitute a funds transfer under the EFTA and Regulation E. But even with such transfers, as Mann notes, it is unclear to what extent a transfer initiated by an interloper who gained access a consumer’s P2P account and authorized a transaction would be treated as unauthorized under Regulation E (assuming that a customer had given his access code to the P2P intermediary). In this instance, the transfer, if erroneous (because unauthorized), might not qualify for error resolution.\textsuperscript{38}

\textsuperscript{35} Id. \textsuperscript{12f(iv)}.
\textsuperscript{36} Id. \textsuperscript{12h(i)}.
\textsuperscript{37} Id. \textsuperscript{12h(iii)}.
\textsuperscript{38} Mann, supra note 17, at 697. As Mann states:
The only ambiguity applies if the interloper uses the information to withdraw funds from the consumer’s deposit account. In that event—because of an odd glitch in the regulation—it seems that neither the P2P provider nor the bank is obligated to return the funds to the consumer’s deposit account. The bank apparently is not obligated because it is entitled to treat the transaction as authorized. A transaction is authorized under the EFTA if it is executed by a party (the P2P provider in this case) to whom the consumer has given the relevant access information. Because that fact makes the transaction “authorized” with respect to the account from which funds were drawn, it appears that the rules related to “unauthorized” transactions impose no obligation on the P2P provider for the loss. The most likely source of recovery for the consumer would be an action against the P2P provider’s depository institution (the entity that originated the ACH transfer) for a breach of the applicable National Automated Clearing House Association (NACHA) warranties. Because of the limited litigation to date in that area, it is difficult to assess the likelihood of prevailing in such an action. 
\textit{Id}. at 696 (citations omitted).
This suggests that there are aspects of PayPal's payment mechanisms that do not clearly qualify for traditional regulatory coverage, even when PayPal has chosen to offer the same rights to its users. This may include situations where a consumer has used a credit card to make a payment but PayPal is the merchant of record rather than a seller. In such instances, Regulation Z chargeback rights may not exist between the User as a buyer and the seller who ultimately receives payment from PayPal. In other instances, a funds transfer may not qualify as an electronic funds transfer subject to Regulation E. PayPal does provide for error resolution procedures in its user agreement that comply with Regulation E procedures.  

2. Electronic Bill Presentment and Payment

The second type of emerging payments method that has caused some regulatory uncertainty is Electronic Bill Presentment and Payment (EBPP). An EBPP service pays bills directly from a customer’s bank account or by charging a consumer’s credit card. Such services may be offered in differ-

39. *PAYPAL*, supra note 16, at ¶ 12.2–12.3, 12.5. The User Agreement reads:

Notifying PayPal of Errors and/or Unauthorized Transactions. To notify us if you believe there has been or will be an error or unauthorized transaction on your Account, [contact us by telephone, by using this online report form, or in writing]. If you initially provide information to us via the telephone, we may require that you send your complaint or question in writing within 10 Business Days after the phone contact. Please complete the affidavit form and submit it online or mail it to PayPal....

Review of Reports of Errors and/or Unauthorized Transactions. We will advise you of the results of our investigation within 10 Business Days after we receive your notice (or 20 Business Days for transactions done at a point of sale terminal or outside the United States). If we have made an error, we will correct it promptly. If we need more time, however, we may take up to 45 Days to investigate your complaint or question (and 90 Days for transactions made at a point of sale terminal or outside the United States). If we decide that we need more time, we will provisionally re-credit your Account for the amount you think is in error within 10 Business Days after we receive your notice; so that you will have use of the money during the time it takes us to complete our investigation. If you initially provided information to us via the telephone and we do not receive your complaint or question in writing within 10 Business Days after your oral notice, we are not required to provisionally re-credit your Account.

....

Errors. If we discover a processing error, we will rectify the error. If the error resulted in your receiving less money than you were entitled to, PayPal will credit your Account for the difference. If the error results in your receiving more money than you were entitled to, PayPal may debit the extra funds from your PayPal Account. If the error resulted in our not completing a transaction on time or in the correct amount, we will be liable for your losses or damages directly and proximately caused by this failure, unless:

a. through no fault of ours, you did not have enough available funds to complete the transaction,

b. our system was not working properly and you knew about the breakdown when you started the transaction, or

c. circumstances beyond our control (such as fire or flood or loss of Internet connection) prevented the transaction, despite our reasonable precautions.
ent formats.\textsuperscript{40} One such format is a situation where a “biller” (e.g., a merchant or a public utility) offers consumers the opportunity to visit a biller-operated website, and to authorize payment via credit card, debit card, or ACH transfer (debit or credit).\textsuperscript{41} With respect to “biller” web sites, errors may arise if a biller accesses a consumer’s account and pays another customer’s bill or pays itself for a bill that the consumer did not authorize.\textsuperscript{42} A second type of bill payment service is offered by financial institutions. A consumer can direct his or her bank, for example, to pay bills on a one-time or a recurring basis using ACH transactions.\textsuperscript{43}

The third type of EBPP service is offered by non-bank entities, sometimes referred to as lockbox providers.\textsuperscript{44} Companies such as CheckFree allow consumers to register to pay bills from multiple companies through one portal. With such a service, a consumer logs onto CheckFree’s website and accesses her CheckFree account to view bills, which have been presented by multiple billers.\textsuperscript{45} A consumer can direct CheckFree to make payments to different billers on her behalf. CheckFree will then initiate a funds transfer out of a consumer’s bank account in order to pay the biller. Alternatively, a consumer may choose to pay a bill with his or her credit card. The EBPP transactions that occur are typically covered by Regulation E.\textsuperscript{46}

With a non-bank EBPP provider, there may be errors that arise which are not covered by Regulation E. Consumers may pay erroneous or fabric-
A consumer may pay a bill that is either created by a third party interloper or that is erroneously posted to his account. In either scenario, the consumer still “authorizes” the payment transfer, having been duped by the interloper or unaware that he received a bill in error. In these circumstances the transaction may neither be unauthorized nor qualify as an error.

In addition, there are situations when an EBPP provider makes a payment on behalf of a consumer to a merchant, but does so by generating a check image (a remotely created check) or by debiting a consumer’s account (which would be a funds transfer) and then paying the merchant with a traditional paper check. In this case, the payment of the merchant by check would likely qualify as a funds transfer if the original payment request were made by computer, unless a customer’s financial institution notified the customer that payments to a specific payee or payees would be made only by check.

While this may not be common, a company such as CheckFree reserves the right to make a payment by this method. A consumer may be expecting that his payment will be made with a funds transfer, when in fact the payment was converted at the discretion of an EBPP provider. Perhaps a particular merchant cannot receive an ACH payment or, for another reason, a check must be sent in lieu of a transfer. If a consumer is provided with notice of this practice, the transaction will fall outside of Regulation E and perhaps back into ordinary contract.

CheckFree is one of the largest non-bank EBPP providers. As part of its user terms and conditions, it provides a ninety day window in which a consumer must report an error to his or her bank account. The terms state: “If you think your financial institution statement is incorrect or you need more information about a Service transaction listed on the statement, we must hear from you no later than ninety (90) days after the FIRST statement was sent to you on which the problem or error appears.” The error

47. For a lengthier discussion of these types of errors, see Mann, supra note 17, at 699.
48. As at least one commentator has noted, “Presumably since computer initiated payments are covered by the regulation, such payments (even if made by paper instrument) are protected by the error resolution requirements of Section 205.11.” Spiotto, supra note 40, at 16 n.49; see also Electronic Fund Transfers, 66 Fed. Reg. 15,187, 15,193 (Mar. 16, 2001) (stating that section 205.3(b) covers a “payment made by a bill payer under a bill-payment service available to a consumer via computer or other electronic means, unless the terms of the bill-payment service explicitly state that all payments, or all payments to a particular payee or payees, will be solely by check, draft, or similar paper instrument drawn on the consumer’s account, and the payee or payees that will be paid in this manner are identified to the consumer”).
resolution procedure itself mirrors Regulation E. Of course, a customer should typically contact his or her bank or financial institution to pursue a Regulation E error.

B. Scenario Two: Electronic Check Conversion and Substitute Checks

If a consumer pays a bill with a paper check, that check may eventually be processed in one of three ways. The original processing and collection of a check is governed by the Uniform Commercial Code. If the check is converted by a merchant, however, it may be converted into an electronic funds transfer subject to Regulation E. Finally, if a check is processed through electronic image exchange, a consumer will not receive his original check back but rather a “substitute check.”

Electronic check conversion relates to checks being converted by payees and turned into electronic funds/ACH transactions. Until recently, it was unclear whether such transactions were governed by Articles 3 and 4 of the U.C.C. or by Regulation E. One relevant type of conversion involves conversion at the point of sale or purchase. With a point-of-purchase (POP) entry, a merchant takes a consumer's check, marks it “void,” and hands it back to the consumer. At that point, the check is processed as an

49. In the event of an error or if the customer has a question, CheckFree requires the following: You must:
1. Tell us your name and Service account number;
2. Describe the error or the transaction in question, and explain as clearly as possible why you believe it is an error or why you need more information; and,
3. Tell us the dollar amount of the suspected error.

If you tell us verbally, we may require that you send your complaint in writing within ten (10) Business Days after your verbal notification. We will tell you the results of our investigation within ten (10) Business Days after we hear from you, and will correct any error promptly. However, if we require more time to confirm the nature of your complaint or question, we reserve the right to take up to forty-five (45) days to complete our investigation. If we decide to do this, we will provisionally credit your Payment Account within ten (10) Business Days for the amount you think is in error. If we ask you to submit your complaint or question in writing and we do not receive it within ten (10) Business Days, we may not provisionally credit your Payment Account. If it is determined there was no error we will mail you a written explanation within three (3) Business Days after completion of our investigation. You may ask for copies of documents used in our investigation. The Service may revoke any provisional credit provided to you if we find an error did not occur.


ACH electronic transfer, which moves funds out of the consumer’s bank account.\textsuperscript{52}

A second situation involves checks mailed to billers, often credit card companies. The biller receives the check which has been sent to a “lock-box” where the check is scanned and retained. The check is not sent on for collection, however. The check payment is converted to an ACH transfer.\textsuperscript{53} NACHA refers to this as an Account Receivable Conversion (ARC) entry. In both of these situations, a consumer thinks he or she is sending in a check for payment and is instead submitting to an ACH funds transfer.

The Federal Reserve Board has made it clear that Regulation E applies to electronic check conversion transactions.\textsuperscript{54} Before this clarification, it was unclear to what extent Regulation E applied and what obligations, if any, merchants had to obtain authorization from consumers before converting their checks into funds transfers. The Regulation E amendments also made it clear that merchants were covered by Regulation E for the limited purpose of having to give consumers notice of when their check was being converted.\textsuperscript{55}

While most electronic check conversions are covered by Regulation E, not all are. This leads to a divergence in treatment for payments that may

\textsuperscript{52} For a useful description, see Stephanie Heller, \textit{An Endangered Species: The Increasing Irrelevance of Article 4 of the UCC in an Electronics-Based Payment System}, 40 Loy. L.A. L. Rev. 513, 516–20 (2006). This type of transaction is referred to as a point-of-purchase (POP) ACH entry. \textit{Id.} at 517–18.

\textsuperscript{53} \textit{Id.} at 519 (discussing an ARC).

\textsuperscript{54} Electronic Funds Transfers, 71 Fed. Reg. 1638, 1659 (Jan. 10, 2006) (codified at 12 C.F.R. § 205.3(b)(2)(i)). As Heller notes, similar guidance was previously provided in the official commentary to Regulation E. Heller, \textit{supra} note 52, at 523 & n.50; see also Electronic Fund Transfers, 66 Fed. Reg. 15,187, 15,187–89 (Mar. 16, 2001) (“Under the final rule, where a consumer authorizes a one-time EFT from the consumer’s account using information from a check to initiate the transfer, the transaction is covered by Regulation E. Application of the rule is consistent and the result is that whether the check is blank, partially completed, or fully completed and signed; after the check is presented at POS or mailed to a merchant or lockbox and later converted to an EFT; or whether the check is retained by the consumer, the merchant, or the merchant’s financial institution. … The final rule provides that where a consumer authorizes the use of a check for initiating an EFT, the transaction is not deemed to be originated by check. The transaction is covered by Regulation E. … In the context of check conversion, authorization takes place if the consumer engages in the transaction after receiving notice that the transaction will be treated as an EFT.”).

\textsuperscript{55} As the Federal Reserve Board indicated:

among other things, the final rule announced today provides that merchants and other payees that convert payments by check into electronic fund transfers must provide a notice to consumers to obtain consumer authorization for the electronic fund transfer. Merchants and other payees must also notify consumers that if a check is converted, funds may be debited from consumers’ accounts as soon as the same day that payment is received, and the check will not be returned by their financial institution.

be processed in the same manner, and may also lead to consumer confusion as to what will happen to the instrument. For example, not all checks are eligible for conversion under the NACHA rule.\textsuperscript{56} Moreover, when a merchant or payee initiates an electronic funds transfer in error, the transaction is not covered by Regulation E. For example, when a payee mistakenly initiates an electronic check transaction, such as when a payee attempts to convert a money order, such transactions are not subject to the EFTA even if initiated as an electronic check transaction.\textsuperscript{57} Thus, a consumer might produce a negotiable instrument at the point of sale, see it converted, and believe that it is now being treated as an electronic funds transfer or ACH transaction. In fact, the transaction will still be governed by the Uniform Commercial Code.\textsuperscript{58}

If a check is treated as a check rather than as an ACH transaction, the legal consequences to the consumer are significant. Article 4 of the U.C.C. provides very different rights to a consumer than does Regulation E, including differences in the timeframe in which a payor must notify his bank about an unauthorized payment and differences in error resolution timeframes. Also, under Article 4, a consumer has no right of provisional recredit under U.C.C. section 4-406 as compared with Regulation E.\textsuperscript{59}

Electronic check conversion is one example of payment convergence. Merchants and billers can quickly convert a check governed by one set of rules into an electronic funds transfer, which is governed by a different regime. When a consumer pays by check, there is no certainty as to what the outcome will be in terms of rules and protections.

In the end, there is still uncertainty as to which method might be used when a consumer initiates a transaction by a check. And the method that is chosen by the merchant or the financial institution will drive a consumer’s remedy. In theory, consumers should receive notice when a conversion of their check occurs, but this notice may not be effective or highly visible.\textsuperscript{60}

\textsuperscript{56} Heller, supra note 52, at 523 & n.53 (explaining that under the NACHA operating rules checks must conform to certain requirements, e.g., checks must be for amounts less than $25,000).

\textsuperscript{57} Electronic Funds Transfers, 71 Fed. Reg. 1638, 1645 (Jan. 10, 2006) (discussing the issue of transactions initiated by mistake).

\textsuperscript{58} Heller, supra note 52, at 524 ("[I]f an item that was ineligible for conversion is nevertheless converted or where a court (or jury) determines that authorization to convert a check to an ACH debit entry was never obtained, a significant exception to this rule may result. In such instances, Article 4 may well apply, at least with respect to the rights of the drawer, despite the fact that the check was 'collected' through the ACH network.").

\textsuperscript{59} \textit{See also id.} at 524 n.57.

\textsuperscript{60} Hearing, supra note 50, at 57 ("If a business wants the option of processing a check under the ARC rules, Reg. E. . . requires the businesses to notify consumers that their checks may be processed electronically. Two of my credit card companies provide that notice. One has it buried in a very long dense paragraph that addresses many topics having nothing to do with ARC. The other company has the
Moreover, while Regulation E does provide consumers with better remedies, a consumer may prefer to have a paper check processed because of the longer time it takes for check collection.

Are consumers aware of check conversion and whether it will change their substantive legal rights? Check conversion, of course, accelerates the clearing process for a consumer’s payment, and thus reduces the float because the consumer’s account will be debited the same day or the next day. According to a recent study by the Federal Reserve of Boston, few respondents in a study (who were Federal Reserve employees) who were presented with the option of check conversion would alter their payment behavior. Only 10% stated they would alter their behavior for Lockbox/ARC conversion and 27% for POS conversion. Both percentages were lower than the 31% of respondents who were asked about changing their payment behavior if they were to lose their float. Therefore “either the respondents were unaware that check conversion reduces float or other factors restrained their actions (or both).”

The Boston Federal Reserve also asked about whether a consumer’s knowledge of ARC procedures might change consumer behavior. As of June 2004, under NACHA rules, “companies were ‘strongly encouraged’ to notify U.S. consumers of their right to ‘opt out’ of conversions of checks to ARC and to provide information on how to do so.” Therefore, the Boston Fed asked consumers about whether they would exercise this right “under the circumstances.” Approximately half said they would not opt out, 38% were uncertain (which may mean they did not understand) and 13% said they would opt out. The most common reasons respondents gave for opting out of ARC were “check return, float benefits, and concerns about errors.” As the Boston Fed pointed out, however, opting out is an active and time-consuming process requiring notice to the originator of the ARC. Some respondents that did change their payment method substituted debit for check conversion and online bill payment for check with ARC.

notice in the portion of the statement that I return when I pay the bill. Consequently, I have no record of that notice to refer to once I mail the payment.”)

62. Id.
63. Id. at 46.
64. Id.
65. Id. at 47.
In addition to electronic check conversion, Congress recently enacted the Check Clearing for the 21st Century Act ("Check 21"), which became effective in October 2004. Mark Budnitz has noted that check substitution under Check 21 further muddies the waters with respect to check conversion.\(^{66}\) Check 21 makes it easier for banks to electronically transfer check images instead of physically transferring paper checks by permitting banks to replace original checks with "substitute checks."\(^{67}\) Substitute checks are special paper copies of the front and back of the original check. They can be processed as if they were original checks. The front of a substitute check should state: "This is a legal copy of your check. You can use it the same way you would use the original check."\(^{68}\) A consumer can use a substitute check as proof of payment, just as he would use an original check.

If a consumer receives a substitute check rather than his original check (or other type of copy) and there is a problem or error with the check that causes a consumer to lose money, Check 21 provides a special procedure that permits a consumer to seek a refund (called an "expedited recredit"). This special procedure applies to substitute checks only.

Regulation E provides for a sixty-day window within which a consumer must report an error; Check 21 provides for a forty-day window if a substitute check is provided to the consumer and the consumer wants a recredit. The U.C.C. does not have any specific duties to investigate or credit within its provisions. Of course, a consumer could sue to compel a bank to investigate, and this might be considered a breach of the bank's duty of care or an act in bad faith. If a consumer receives his original paper check, the deadline for reporting an error will be specified in the account agreement and can be as short as two weeks.\(^{69}\) As Budnitz notes, "the Electronic Funds Transfers Act and Check 21 provide consumers with a reasonable non-litigation remedy."\(^{70}\) The U.C.C, however, does not.

C. Scenario Three: Stored-Value and Prepaid Cards

A third category of emerging payments that poses regulatory uncertainty is stored-value and prepaid cards or accounts.

\(^{66}\) Budnitz, supra note 10, at 254–55; see also Hearing, supra note 50, at 56.


\(^{69}\) Hearing, supra note 50, at 56.

\(^{70}\) Id.
In 1996, the Federal Reserve Board noted that if stored-value cards were not covered by Regulation E "consumers might regard off-line accountable stored-value products as comparable to debit or credit cards, and thus might expect similar rights and remedies to apply." This may relate to the fact that consumers have expectations that are developed as a result of their long term usage of credit cards and debit cards. To the extent that stored-value cards replicate other payment methods (e.g., in the use of a plastic card or a POS device), consumers may believe that certain protections accompany their use of a prepaid card.

During the 1990s, stored-value products were an innovation in payment systems technology. Today, stored-value products are often referred to as "prepaid" cards, referring to the fact that consumers pay value up front to purchase a card. The card is often used to pay for goods or services from a merchant or a host of merchants. The terms "stored value" and "prepaid," while often used interchangeably, can also be used to signify different concepts. The term "stored value" is often associated with products for which prefunded value is recorded onto a payment instrument. The term "prepaid" is associated with products for which prefunded value is recorded on a remote database, which must be accessed for payment authorization. The term "prepaid" describes most of the products on the market today and is used more widely in current literature.

There are different types of stored-value or prepaid cards. Some cards are part of so-called "closed" systems, in which a consumer can use a card for a limited range of goods or services, typically provided by one merchant or one issuer. An example of a closed system would be a university photocopy card or a subway system metro/transit card. In these examples, a stored-value card can be used to purchase a narrow basket of services. At the university, a student would use his photocopy card to make copies in...
the library. A subway rider would use his or her card for riding on the subway and perhaps also on a city bus.74

“Open” systems are systems in which a stored-value card may be used as a cash substitute. The card is widely accepted by merchants and vendors in lieu of physical cash. An example of an open system would be a stored-value or prepaid debit card, in which the consumer may use the card at a wide range of merchants to pay for a large universe of goods and services. Some commentators make a distinction between open prepaid cards that operate as debit or ATM cards and prepaid purchasing cards that can be used widely throughout a country to purchase goods or services only, but are not redeemable as cash. Such cards are also referred to as universal gift cards.75

“Mixed” or “semi-closed” systems are ones that have features of open and closed systems. A stored-value gift card program offered by a shopping mall might be an example of a mixed system. For example, a stored-value gift card might be accepted by multiple merchants within a shopping mall. This system is not entirely closed, because a wider array of merchants has agreed to accept the card as a means of payment. At the same time, the system is not open, as the card may have no use outside the walls of the shopping center.76

In 1994, the Federal Reserve Board first contemplated whether Regulation E should apply to stored-value cards. The proposal generated a large number of comments, and the Board prepared an analysis of stored-value products and their treatment under Regulation E. Based on this analysis, the Board proposed new amendments to Regulation E in May 1996.77 This proposed rule would have exempted many stored-value products, while others would have been covered under limited requirements. In 1996, the Federal Reserve Board did consider extending the application of Regulation E to stored-value cards more generally. The proposed amendments to Regulation E carved out a de minimis exception for cards issued for less than $100.78

76. Id. at 58; Furletti, supra note 73, at 2–4.
78. Id. at 19,701; see also Sean M. O’Connor, The De Minimus Exemption of Stored Value Cards from Regulation E: An Invitation to Fraud?, 5 RICH. J.L. & TECH. 6 (1998), http://law.richmond.edu/jolt/v5i2/oconnor.html.
The Federal Reserve proposed to apply a *de minimis* exception to off-line accountable and online stored-value systems capable of storing only up to $100. Offline unaccountable stored-value systems were excluded from the proposed amendment.79 In the comments accompanying the proposed amendment, the Board justifies the *de minimis* exemption by simply stating that "[f]or a stored-value product limited to a relatively small amount of funds, the amount at risk would be sufficiently minimal that application of even modified Regulation E protections appears unnecessary."80 A final rule was never published.

Later in 1996, Congress directed the Board to conduct a study evaluating whether provisions of the EFTA should be applied "to electronic stored-value products without adversely affecting the cost, development, and operation of such products."81 In response to this legislative mandate, the Federal Reserve Board issued a comprehensive report in 1997, which considered several approaches for the selective application of Regulation E's protections to electronic stored-value products. At that time, the Board concluded that it was premature to regulate stored-value products, as such regulation might have an adverse impact on innovation in their development.82

At present, if a consumer uses a prepaid or stored-value card, there is no legislatively-mandated error resolution procedure (with the exception of payroll cards). As some have noted, prepaid cards may be targeted at members of vulnerable populations, who would benefit from having specific error resolutions in place, as contrasted with pure contract remedies.83 Payroll cards are subject to Regulation E as of July 2007.84 This is not to say that prepaid cards other than payroll cards offer no consumer error resolution features. Branded cards (prepaid debit cards, for example) offer protections that mimic Regulation E through card association network rules,
which provide more generous error resolution timeframes of up to 120 days.85

Consumers may expect that such prepaid cards will operate like traditional debit cards, given their branding (e.g., as MasterCard or Visa prepaid cards), their name (sometimes referred to as prepaid debit cards) and their functionality (use at a POS terminal, for example, where credit and debit cards are also swiped).86

Under a Federal Reserve Board Interim Final Rule, nearly all the provisions of Regulation E apply to payroll cards—with some important modifications.87 The main modification is that employers or others providing payroll cards need not provide a printed periodic statement to employee cardholders.

A new § 205.18 of Regulation E provides financial institutions flexibility in providing account information to consumers. Financial institutions may elect to provide periodic statements under § 205.9 as they would for other accounts. As an alternative, however, institutions may instead:

(1) Make balance information available through a readily available telephone line; (2) make available an electronic history of the consumer’s account transactions, such as through an Internet web site, that covers at least 60 days preceding the date the consumer electronically accesses the account; and (3) provide promptly upon request a written history of the consumer’s account transactions, covering at least 60 days preceding the date the institution receives the consumer’s request.88

Section 205.18(c)(4) establishes a rule for when the sixty-day period for reporting an error begins for purposes of Regulation E error resolution. The reporting period will be based upon how a consumer has obtained the account transaction history on which an error appears. A financial institution must comply with the error resolution procedures set forth in § 205.11 once the consumer reports the error in her account transaction history within the requisite sixty days. The sixty-day rule is measured in one of two ways:

[I]f a consumer obtains transaction information electronically under § 205.18(b)(1)(ii), the 60-day period for reporting an error begins on the

85. Furletti, supra note 2, at 21 (stating that “most issuers explicitly provide strong error-resolution protection for at least” sixty days).
86. For an interesting presentation that poses questions about regulation and different types of stored value, see Sherrie L.W. Rhine, Sr. Economist, Fed. Reserve Bank of N.Y., Presentation at the 15th Annual Nat’l Consumer Protection Week Conf.: Stored Value Cards, Not Credit, Not Debit, What Are They? (Apr. 26, 2005), slides available at http://www.bos.frb.org/consumer/conf/ncpw/2005/svc.pdf (posing question as to whether consumers know that some stored-value cards have limited or no consumer protections).
88. Id. at 51,443.
date the account is electronically accessed by the consumer. If the con-
sumer requests a written history of transactions under § 205.18(b)(1)(iii),
the 60-day period begins on the date the institution sends the written his-
tory. A consumer is deemed to electronically access an account once she “enters
a user identification code or a password or otherwise complies with a secu-
rity procedure used by an institution to verify the consumer’s identity.”

The periodic statement requirement is an important aspect of Regula-
tion E’s consumer protections. Consumers’ duty to report errors is linked to
receipt of their bank statement. When the Board considered whether to
extend Regulation E requirements to Electronic Benefits Transfer programs
in 1994, it carved out an exception to the requirement that financial institu-
tions provide a periodic statement to consumers. With EBT transfers, fi-
nancial institutions would not need to provide a periodic statement if: “(1)
account balance information is made available to benefit recipients via
telephone and electronic terminals and (2) a written account history is
given upon request.” With payroll cards, the Board chose to replicate the
same periodic statement exceptions it had applied in the case of EBTs.

The Federal Reserve Board revisited the issue of whether to extend
Regulation E to all stored-value/prepaid card products or a broad class of
general purpose prepaid cards, and some consumer group commentators
urged the Board to apply Regulation E to all card products to which an
individual might transfer some portion of his or her wages, even if such
cards are not “payroll card accounts” offered by an employer. These
commentators asserted that such general spending cards are marketed as account substitutes and therefore should be covered under Regulation E.\textsuperscript{94}

Consumer groups also encouraged the Board to regulate stored-value products that might store important household assets, such as workers compensation, unemployment benefits, or tax refunds.\textsuperscript{95} Ultimately, the Board did not expand the scope of the interim final rule beyond payroll cards.\textsuperscript{96} As the Board noted, it will monitor the development of other card products and may reconsider regulation in the future.\textsuperscript{97}

Do stored-value/prepaid card issuers offer their users any error resolution features? This varies. One important question, of course, is whether a particular card is accountable either online or offline. On the one hand, branded prepaid cards are subject to network rules such that there is an error resolution procedure that is part of the card-processing system.\textsuperscript{98} The

\begin{flushright}
\end{flushright}

\textsuperscript{94} Letter from Consumers Union, supra note 93, at 4.

\textsuperscript{95} Id. at 5.

\textsuperscript{96} The Federal Reserve Board of Governors stated:

Payroll cards are established directly or indirectly by an employer for the express purpose of receiving on a long-term basis, recurring payments of a consumer's wages, salary or other compensation. Accordingly, there is a greater likelihood that the account will serve as a consumer's principal transaction account, and hold significant funds for an extended period of time. In contrast, general spending cards are established by the individual consumer, and while the consumer might choose to deposit some portion of salary (as well as other funds) onto a general spending card, the consumer also may use these products like gift cards or other stored-value or prepaid cards. Under the latter situation, consumers would derive little benefit from receiving full Regulation E protections for a card that may only be used on a limited, short-term basis and which may hold minimal funds, while the costs of providing Regulation E initial disclosures, periodic statements and error resolution rights would be quite significant for the issuer. In addition, coverage of such products could impede the development of other card products generally. Similarly, although some card products may be used to transfer significant or important sums to a consumer, these products are generally designed to make one-time or a limited number of payments to consumers, and are not intended to be used on a long-term basis. Given these above considerations, the Board has determined to limit the scope of the interim final rule to payroll card accounts. The Board will monitor the development of other card products and may reconsider Regulation E coverage as these products continue to develop.

\begin{flushright}
\end{flushright}

\textsuperscript{97} Id.; Donald J. Mosher & Joshua H. Kaplan, Payroll Cards and Regulation E, 2 J. PAYMENT SYSTEMS L. 583, 591 (2006).

\textsuperscript{98} For example, the Prepaid Visa RushCard, which was branded by rap producer Russell Simmons, provides the following procedure in the event of errors or questions about a card transaction:

\begin{itemize}
  \item Call or write to Customer Service as soon as you can, if you think your Card Balance is incorrect or if you need more information about a transaction . . . .
  \item Whether calling or writing you must: (a) tell Customer Service your name and Card number; (b) describe the error or the transfer you are unsure about, and explain as clearly as you can why you believe it is an error or why you need more information; (c) tell Customer Service the dollar amount of the suspected error.
\end{itemize}
Starbucks card, which is a more limited purpose or closed system, but is accountable online if card holders register, also has an error resolution procedure:

We reserve the right to correct the balance of your Starbucks Card account if we believe that a clerical, billing or accounting error occurred. If you have questions regarding your transaction history or any correction, or if you dispute any transaction or correction that has been assessed against your Starbucks Card, please call our customer service department at 1-800-STARBUC. We will conduct an investigation and communicate the results and correct any error that we verify as soon as we finish the investigation. If no error was found, we will communicate an explanation. We shall have no liability for any billing error unless you provide us notice within sixty (60) days of the date of the transaction in question. You should monitor your transactions and account balances closely.

Starbucks does mimic Regulation E in that it requires consumers to notify the company of alleged errors within sixty days of the transaction. This is less generous than Regulation E, which triggers a duty to report sixty days from receipt of a periodic statement, or in the case of payroll cards, after a consumer has accessed relevant transaction information, but makes sense given that this is a card primarily used to purchase coffee and food items. The Wal-Mart gift card, however, does not post any error reso-

If you provide this information to Customer Service orally, you may be required to send Customer Service your complaint or question in writing within 10 business days. Please note that any notice transmitted to any address other than the Customer Service address above, including but not limited to any e mail address or website, will not constitute valid notice. We will tell you the results of our investigation within 10 business days after we hear from you and will correct any error promptly. If we need more time, however, we may take up to 45 days to investigate your complaint or question (90 days if your complaint or question relates to a point of sale transaction or an electronic fund transfer transaction that was started outside any state, territory or possession of the United States, the District of Columbia or Puerto Rico). If we decide to do this, we will re-credit your Card Balance within 10 business days for the amount you think is in error, so that you will have the use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing and we do not receive it within 10 business days, we may not re-credit your Card Balance. If your claim involves an electronic fund transfer associated with your Card that took place within 30 days after its purchase, each 10 business day period referred to in this paragraph will be 20 business days and the 45 day period referred to in this paragraph will be 90 days. We will tell you the results within 3 business days after we finish our investigation. If we decide that there was no error, we will reverse the credit (if any) and send you a written explanation. You may ask for copies of the documents that we used in our investigation.


lution procedures on its web site. Other gift card issuers provide for a shorter period of reporting for error resolution.

II. EXTENDING THE EFTA AND REGULATION E: CONVERGING TOWARDS UNIFORMITY

As stated in Part I, two things are occurring in the consumer payments arena. First, consumers are confused as to their rights and duties with respect to new types of payments as well as mechanisms which may involve multiple channels for processing. Second, payment systems are converging as different actors can convert payments from one form to another. The use of funds transfers is becoming a central piece of how a consumer payment is executed.

At present, error resolution rules are divergent. Checks are not subject to Check 21 and many types of stored-value cards are not subject to error resolution procedures. Moreover, time periods for payment products vary. Credit cards are governed by TILA and Regulation Z and have a sixty-day reporting window. Debit cards are governed by the EFTA and there is a sixty-day window with a right of recredit after forty-five days. Substitute checks have a forty-day window for reporting errors and for seeking recredit. Finally, the U.C.C. is silent and allows banks to impose much shorter time periods by agreement. Is there a sound policy basis, or are the different regimes a product of differing Congresses?

Should there be greater uniformity in error resolution between consumer payment mechanisms? Mark Budnitz has done a thorough job of articulating the problem for consumers with the divergence in rules. As he has noted, “Requiring an error resolution procedure would mainly affect checks not subject to Check 21 and stored value cards.” He advocates for one unified rule setting forth the length of time a consumer has to notify


102. See also Mann, supra note 3, at 634 (providing anecdote of colleague who was unaware of distinction between chargeback rights with credit card as compared with debit card transaction). Mann also notes that “with the debit card market increasingly dominated by the PIN-less debit card markets by Visa and MasterCard, the distinction between the credit card and the debit card is almost invisible to all but the most sophisticated consumers.” Id.

103. Budnitz, supra note 10, at 281.

104. Mann, supra note 17, at 694.

his financial institution of an error. 106 Budnitz further recommend that the recredit rights under the EFTA and Check 21 should be extended to all types of payment systems. 107 But is confusion alone a reason for uniformity? Is there a theoretical argument to be made for greater uniformity?

There are some types of errors that may occur in any payments system, such as duplicate payments, payments made for incorrect amounts, omitted payments, and misdirected payments, to name a few. There needs to be a process for investigating and resolving those errors. As a baseline matter, common error resolution processes may inure to the benefit of consumers and financial institutions alike. Regulation, industry practice, or private rule-making can amplify how investigations should take place with respect to a particular technology. Regulation E sets timeframes within which parties must act and investigate. It does not, however, regulate the nature of the investigatory process.

Critics who oppose extension of Regulation E to other types of prepaid cards note that the full application of Regulation E would be costly—and often, the focus is on the periodic statement reporting requirement. 108 To the extent that Regulation E’s periodic statement requirements are narrowed to require that a consumer have access to transaction information online or via telephone, businesses will have a lower compliance burden than the one faced by banks with respect to debit cards. Moreover, one could lower requirements even further, to require reporting within sixty days of a particular transaction record being made available, as is the case with Starbucks. The Federal Reserve has already eliminated the receipt requirement for funds transfers and debit card transactions under $15. If this requirement were implemented for new types of payments, it would eliminate much of the burden that the industry fears. 109

106. Id.
A factor indicating that the time may be right for expansion of Regulation E’s scope relates to existing market conditions. Branded prepaid cards offer error resolution procedures that resemble those provided under Regulation E. Even closed or mixed system cards, such as the Starbucks card, use processes that mimic Regulation E in terms of timelines for reporting errors. This shows that error resolution procedures are feasible for such types of products. Would it not be better, under those circumstances, to reinforce consumer expectations by mandating a similar error resolution procedure for prepaid cards that are either for general purpose or of a certain value?

It will be helpful for the Federal Reserve to monitor the application of Regulation E to payroll cards. To the extent that the modified notice and reporting requirements are less burdensome, it may be that general purpose card issuers should also be subject to the same rules. Many prepaid card issuers, however, weighed in against the expansion of Regulation E at the time the payroll card regulations were published for comment. To extend the scope of Regulation E further would require an examination of other prepaid card models to see how consumers are using them and when and how errors occur. In the interim, recent studies have shown that cards with a more general or open structure provide error resolution procedures that mimic Regulation E as a matter of industry practice.

Should there be a uniform error resolution standard for all types of consumer payments? What would uniformity do for consumer payments? For consumers, this may reduce confusion and increase the chance of trying new payment products. As Budnitz remarks: “Consumers also need uniform error resolution procedures to prevent undue confusion from the many different types of consumer payments that involve a consumer’s bank account.” If one sets aside stored-value cards, there may be a better case to be made for uniform error resolution mechanisms for debit cards, credit cards, and checks given the way in which these payment methods are converging and being used interchangeably at the point of sale.

While a lack of regulation may foster innovation, uniformity of consumer protections may also encourage consumer adoption of new payment methods. To the extent that uniformity exists with respect to error resolution, this may incentivize consumers to behave in a predictable and uniform manner with respect to any and all of their payment choices. This, in turn,

110. Budnitz, supra note 10, at 257.

111. Credit card error resolution is currently governed by Regulation Z, which includes a fair credit billing dispute resolution procedure. 12 C.F.R. § 226.13 (2007).
may provide for greater efficiency in consumer reporting and detection of errors. If a consumer knows she has sixty days to detect and report a payments error, for example, irrespective of the method she uses, she may be more vigilant in checking her periodic statements or other transaction records, creating a culture of responsibility.

Is consumer confusion enough to justify uniformity? Surely not. But when confusion is accompanied by convergence, the answer may change. It may be more efficient now to mandate a universal rule, which allows different payment systems to piggyback on one another, or to allow different parties to convert transactions as is the case with electronic check conversions. When consumers are confused, industry players, especially non-banks, are also confused. Trying to craft uniform but less burdensome processes may provide for an efficiency and predictability that will help new entities compete and offer consumers a familiar type of error resolution process.

The expansion of Regulation E/EFTA provisions to payroll cards and to check conversions is one step towards uniformity and harmonization. The EFTA error resolution procedures, which apply to a wider range of transactions, could serve as a useful model for other payment systems. The procedures would need to be modified in some respects, especially with respect to the issue of periodic statement reporting.112

Is uniformity desirable? Peter Alces and others have written about the desirability of uniformity in payments law, but have also criticized previous attempts to harmonize payments law with something like a Uniform New Payments Code (UNPC).113 Alces’s critique focused on issues such as stop payment and reversibility under the UNPC. He did, however, note that effective codification of payment law involves “the identification of common denominators in seemingly different systems.”114

Clayton Gillette has also examined the discrepancies for checks and credit cards when dealing with fraud in payment systems.115 Gillette notes that “[p]recise risk allocations create clear liability rules that minimize the

114. Id. at 103.
115. Gillette, supra note 13, at 184.
cost of the enforcement process . . . [and] facilitate coordination by ensuring that transactors follow similar patterns of behavior.”

As Ronald Mann has described, payments law must resolve four fundamental issues: who bears the risk of unauthorized transactions, how error claims should be resolved, when payments are made so as to discharge the underlying liability, and when payments can be reversed. In his view, the distinction between the first three questions and the fourth is that the first three “should be resolved based on the nature of the underlying technology.”

As for error resolution, the types of situations that are likely to cause errors, as well as the mechanisms for detecting and responding to errors, are likely to “depend on the technology used to clear and process payments.” Therefore, it would make sense that there would be a different rule for those transactions that are processed electronically from those that are processed solely by paper. Mann notes, however, that the move from paper to electronic processing might well eliminate any meaningful difference. At present, the move toward check substitution and conversion means that more transactions are processed electronically. Given this convergence, uniform error resolution may be desirable.

To the extent that the payments in question are also taking place over similar networks (with the exception of some checks that are not converted), it may well make sense to create operator incentives to make advances in technology that will avoid or detect error. As Mann notes, in our legal system regulators have taken the view that for most high technology payment systems, it is appropriate to allocate the risk of loss to the system operator. He argues that it would be more sensible to develop rules for

---

116. *Id.* at 186.
118. *Id.*
119. *Id.* at 639.
120. *Id.*
121. *Id.*
122. There are also moves to convert some electronic payments into checks and to process them accordingly. This demonstrates that payment systems are becoming more interdependent, as conversion occurs in both directions with respect to checks and funds transfers. One example is the Deposited Check Truncation (DCT) pilot, recently announced by NACHA. The DCT pilot will use the ACH network to collect low-value consumer checks. Unlike the current ACH check conversion services (e.g. POP and ARC, which are viewed as electronic fund transfers under Regulation E), NACHA intends the collection and return of checks in the DCT scheme to be governed by traditional check rules under the U.C.C. (except as varied by agreement of the participants under the pilot rules). *See* Press Release, Nat’l Automated Clearing House Ass’n, DCT Pilot Set to Launch 1st Quarter 2008, http://dct.nacha.org/.
123. Mann, *supra* note 3, at 638.
fraud and error resolution "justified by the fact the transactions are processed and cleared in an electronic way."\textsuperscript{124}

This article focuses on the issue of error resolution—whether we can impose a uniform standard across payment systems.\textsuperscript{125} Consumer confusion, to the extent it exists with respect to retail payments, may indicate market failure. As Robert Cooter and Ed Rubin have noted:

\begin{quote}
[I]n an operating market, private agreements between parties will generally produce economically efficient results without the need for legal intervention. Intervention becomes necessary, however, when the market fails to produce these efficient results on its own. Rules that are designed to achieve economic efficiency in payment law, therefore, should enforce agreements between private parties when no market failure has occurred. When market failures exist, legal rules can improve upon private agreements if they are designed with the goal of minimizing costs in mind.\textsuperscript{126}
\end{quote}

As they have also pointed out, disproportionate negotiation costs and asymmetric information create market failures in the allocation of fraud, forgery, and error losses in consumer payment contracts.\textsuperscript{127} When there is market failure, regulatory solutions are often needed to bridge the gap and rectify any inefficiencies. Efficient legal rules assign liability to whichever transacting party can reduce losses at the lowest cost.\textsuperscript{128} As Cooter and Rubin point out, "Recent technological innovations, such as automated check processing, have altered the cost of precaution and will continue to do so in the future."\textsuperscript{129} Thus, while the loss might be allocated to financial institutions and other payments providers, it would follow that there should be an error resolution process in place, which would require the institutions to take steps in a timely fashion. Error resolution becomes an intrinsic part of any efficient loss-allocation scheme.

Cooter and Rubin have concluded previously that "the allocation of fraud, forgery and error losses in consumer payment contracts provides a clear case of market failure."\textsuperscript{130} If the allocation of losses is a situation of market failure (i.e., the market has not provided a rational system of loss

\begin{itemize}
\item \textsuperscript{124} \textit{Id.} at 639.
\item \textsuperscript{125} See also Budnitz, supra note 10, at 257 (stating that in addition to uniform notice requirements, consumers also require uniform error resolution procedures).
\item \textsuperscript{127} \textit{Id.} at 69.
\item \textsuperscript{128} \textit{Id.} at 73–78.
\item \textsuperscript{129} \textit{Id.} at 74–75.
\item \textsuperscript{130} \textit{Id.} at 69.
\end{itemize}
COHERENCE IN ERROR RESOLUTION

allocation), one could extend that to the procedural framework in which the loss allocation takes place.

Consumers are likely to be unaware of the procedures that need to be invoked in order to exercise remedies that are afforded to them because of disproportionate costs of exercising their rights and asymmetric information (e.g., they neither actively negotiate the terms of their service agreements with payments providers nor review such agreements once executed). Individual consumers will typically not expend the time and effort to identify and understand the specific terms of the account agreement with their financial institutions. Cooter and Rubin persuasively argue that consumers do not make informed choices about relevant terms when they contract with financial institutions. By contrast, a financial institution will expend considerable effort in formulating an agreement that furthers its own interests.

Another example of market failure relates to funds availability schedules. Prior to the enactment of the Expedited Funds Availability Act, banks did not have to credit, according to any mandatory time schedule, their customers’ accounts for checks that were deposited. There was no built-in incentive for depository institutions to act quickly with respect to funds availability.

The funds availability problem arises, as might be expected, where individual consumers are involved. Very few consumers have their own money managers (those who do are probably not entitled to be called consumers), and only a few more have the expertise to manage their own funds as a business does. The vast majority are ignorant about the issue. They do not know whether their respective banks allow interest to accrue from the time of provisional credit or rather postpone the accrual of interest until final payment. Similarly, they are not aware of hold policies until confronted with an immediate problem of liquidity. They are thus incapable of evaluating differential bank performance, which gives banks no incentive to compete or otherwise make concessions to consumer desires. This phenomenon, of course, is known as a market failure—in this case the failure of otherwise competing banks to create a competitive market for funds availability services.

In response to the market failure, Congress enacted the Expedited Funds Availability Act and the Federal Reserve implemented this through Regulation CC. This is an example of an overlay of federal law creating a

131. Id. at 68–70 (discussing issues such as the cost of negotiation and asymmetric information between financial institutions and consumers).

132. See id. at 80–81.

process and set of timelines for funds availability.  The EFAA requires a financial institution to disclose its funds availability policy to consumers. The statute also created a mandatory availability schedule. This statute and Regulation CC focus on procedural requirements and leave issues such as the contractual obligation of the parties and the required standard of care to common law.

The issue of funds availability can be compared to the situation of error resolution. Delay in error resolution can benefit a bank or other payments provider, but “the customer is harmed by it. The components of this harm are the reduced access to funds, and, in some cases, monetary costs and personal frustration resulting from accidentally-bounced checks.”

Cooter and Rubin advocate that for funds availability, market-stimulating legislation would be a preferred alternative to the funds availability rules, which they view as market-displacing. With error resolution, it would be difficult to come up with market-stimulating incentives, because error resolution is not “priced” in the way that check collection and processing is. Ultimately, however, Cooter and Rubin viewed the funds availability situation as one where market failure called for some sort of intervention to create better and more efficient methods for check processing and funds availability.

134. See id. at 1130.
135. Id. at 1141-42.
136. Id. at 1154 (“Regulation CC is essentially a set of orders, or commands, and thus follows our traditional model of law. It specifies when funds should be made available (to the extent that this is not already specified in the Act), what should be disclosed, and how such disclosures should be made. It also specifies rules governing notice of dishonor and return, using the same form as standard statutory provisions, but at a level of detail that is generally restricted to administrative regulations. To be sure, many of these rules focus on the sort of operational concerns that the UCC ignores; they deal with mundane matters like the bank’s courier services, the placement of its indorsement stamp, and the precise form of the availability disclosures, rather than the contractual obligations of the parties, their required standard of care and other topics more closely allied to common law. While this reflects the administrative authorship of the rules, the form and structure of these rules differ little from age-old provisions like the Statute of Frauds.”).
137. Id. at 1158-59 (“If customers were wholly rational and had no liquidity problems, they would adjust to delays by holding more money in their accounts. The cost of delayed availability to customers under these conditions would be the value of the cushion that they keep in their accounts to protect against possible overdrafts. The size of this cushion would be determined by two considerations: predictable delay and uncertainty. Predictable delay in processing a check would cause customers to increase their account balances by the instrument’s face value for the duration of the delay (e.g., a delay of two days in processing a $10 check causes account holders to keep an extra $10 in their accounts for two days). Uncertainty would extend the length of time for keeping a cushion in the account. If processing a $10 check will be delayed for at least two days and perhaps by as long as five days, the account holder would keep an extra $10 in the account for longer than two days, but probably fewer than five days.”).
138. Id. at 1178-79.
With respect to error resolution on consumer payments, absent obliga-
tory processes, certain entities do not have to act expediently or efficiently. At the same time, those same businesses can impose quick reporting dead-
lines for consumers with respect to error. Are Regulation E and the EFTA a better way forward?

The EFTA and billing disputes require a financial institution to re-
spond to consumer complaints and to correct the bill or provide an explana-
tion for its refusal to do so. Cooter and Rubin have argued that federal law could be further strengthened and the U.C.C. transformed "if the institution were required to reverse a charge whenever a consumer asserted that it was erroneous." They describe these processes as creating an "obligatory
dialogue between a consumer and the financial institution" such that "[c]onsumers who think the institution has made a billing error are required to notify the institution, and provide the information necessary for the insti-
tution to investigate their claim. The financial institution is then obligated to respond, either by making a correction or explaining why no correction is required."140

This mandatory dialogue, between a consumer and a financial institu-
tion, promotes efficiency and responsible behavior for both parties. A con-
sumer needs to be vigilant at reviewing account statements. Financial
institutions must be vigilant in investigating errors and responding to con-
sumers.

What about the economic aspects of error resolution rules? Cooter and
Rubin also focus on three important considerations when deciding what
type of loss-allocation rules should be deployed for consumer payments:
loss spreading, loss reduction, and loss imposition.141 These factors help to
determine what type of rules will allocate losses in an efficient manner.

With respect to loss spreading, Cooter and Rubin note that the loss-
spreading principle favors assigning liability for a loss to the party that can
achieve risk neutrality at the lowest cost.142 The loss-spreading principle
favors imposing liability on financial institutions that can invest in precau-
tion, innovation, and responsiveness with respect to fraud and error: "For
example, when a bank incorrectly encodes the magnetic numbers on the
bottom of a check, which results in an overpayment, the bank is clearly in
the best position to prevent the loss, because check encoding does not in-

139. Cooter & Rubin, supra note 126, at 116.
140. Id. at 116 n.195.
141. Id. at 70.
142. Id. at 72–72.
volve consumers at all.”143 With respect to loss reduction, banks and other payment providers are cheaper cost avoiders. They can invest in technology that would reduce detect errors.144

If the bank should invest to prevent the loss, should the bank also have an incentive to act to investigate error? In other words, procedural duty to act would further the goals of the loss-imposition principle. Under Article 4, consumers have a duty to act quickly but banks have no corresponding duty. Regulation E requires banks to affirmatively commence error resolution in a timely fashion. Thus, government intervention requires responding to errors, and this in turn may prompt efficiency in error resolution procedures as well as error detection measures.

The loss-imposition principle favors rules where losses are allocated to avoid expensive litigation and to avoid under-enforcement of such rules.145 Thus, this principle favors rules that are simple and clear, such as a strict liability rule with a capped amount of damages.146 In some instances, as Cooter and Rubin point out, this involves rules which require bilateral caution on the part of both parties in a financial transaction. Thus, consumers and financial institutions may both bear some responsibility to take precautions to prevent loss.147 Regulation E requires both the bank and the consumer to act within designated timeframes; if they fail to do so, their claims may be precluded. While the use of procedures from Regulation E does not impose losses on either party, it creates rules that are simple and that emphasize bilateral caution.

Cooter and Rubin have examined transactions which they refer to as “false positive” payments. These are situations where checks are wrongly paid by the bank or paid for the wrong amount.148 Their description of “false positive” payments by a bank replicates a more general category of “errors” which may occur in the retail payments situation—instances where a consumer notices a duplicate payment, overpayment, or an incorrect payment that has been made out of his account. Cooter and Rubin note that financial institutions should be at least partially liable for every loss result-

143. Id. at 76.
144. Id. at 75–77.
145. Id. at 84.
146. Id. at 85.
147. Id.
148. Id. at 86.
ing from a false positive and totally liable for those losses that the consumer cannot efficiently prevent.\textsuperscript{149}

They further indicate that "[t]he current law governing false positives that occur during processing is generally consistent with this rule. If a financial institution pays the wrong person through a processing error, and that person keeps it, the financial institution will be liable."\textsuperscript{150} One other type of processing error can cause either false positives or false negatives. Encoding errors occur when a depository bank encodes the wrong sum in the magnetic numbers placed on the bottom of a check resulting in an overpayment or underpayment to a payee.\textsuperscript{151}

Timeframes can also impact loss allocation, with delay causing as much loss as an incomplete or failed payment.\textsuperscript{152} One answer to this problem may be to establish statutory time limits for payments.\textsuperscript{153} If loss-imposition rules favor placing the loss on the financial institution in those circumstances—the absence of clear error resolution duties and timeframes may weaken this principle. Consumers may underreport errors when there is (i) no clear procedure in place for correcting or investigating error, or (ii) where they are unsure about what rules govern the transaction for which the error occurred.

If Regulation E-type dispute resolution was extended to checks and to all prepaid cards, would this lead to a spike in unwarranted consumer complaints? The answer is likely to be no. In electronic payment systems, repeat offenders (i.e., consumers who intentionally try to "game" the system by filing error reports) can be discovered and their contracts terminated.\textsuperscript{154}

An example of this comes from the credit card sector. As two other commentators, Andrew Morriss and Jason Korosec, point out:

In the payment system context, there are also opportunities for gaming behavior. For example, if a consumer complains about a charge, during the dispute period the amount in dispute is temporarily debited from the merchant's account and credited back to the consumer. This provides the consumer with additional credit, since charges are not applied to the account during the dispute. (Once the dispute is resolved, the temporary debits and credits are either reversed or made permanent.) Consumers who repeatedly game the system, however, self-identify themselves to

\textsuperscript{149} Id. at 90, 97.
\textsuperscript{150} Id. at 111.
\textsuperscript{151} Id.
\textsuperscript{152} Id. at 96.
\textsuperscript{153} Id.
their card-issuer. Since the issuer bears some of the costs from consumer complaints, these consumers’ poor reputation for honesty can be a basis for the issuer to cancel the consumers’ cards. The distinctive feature of card-based payment systems is their ability to make use of the parties’ reputations in controlling attempts to game the system.\footnote{155}

Has the time come to extend Regulation E to other types of payment mechanisms? For example, should the Board regulate general purpose or large sum prepaid cards beyond payroll cards? To the extent that P2P funds transfers out of non-bank accounts are covered, it is hard to distinguish between a prepaid debit card and a PayPal funds transfer. In both, consumers are accessing a funded account (one linked to a device, the other stored online) to pay for goods and services. Mann has argued persuasively about the lack of a real credit/debit distinction. Is there really a distinction to be made between a PayPal account and a prepaid debit card?

Mann argues that the differences between credit card consumer protection and debit card consumer protection “do not map well to the common-sense transactional distinction.”\footnote{156} As he notes, the distinctions only decrease with “the continuing convergence in the functions of the two products.”\footnote{157} Almost half of consumers use their credit card as a “convenience device” and pay off their entire bill every month.\footnote{158} As an illustration, he notes that some credit cards have both credit and debit features, making it “harder to justify the availability of the right to withhold payment turning on the way in which the consumer interacts with the merchant’s payment terminal.”\footnote{159} Mann also notes that some of the distinctions between TILA (or Regulation Z) and the EFTA (or Regulation E) can be explained simply by the fact that two different Congresses enacted these laws and that there is no policy basis for differing definitions of billing errors.\footnote{160}

This article does not address the extension of Regulation E to credit cards, or the expansion of TILA/Regulation Z debit cards or other forms of electronic funds transfers. Ronald Mann has argued persuasively about the lack of importance in the credit/debit distinction and the desirability of expanding TILA coverage to debit card transactions. There also remains a question as to whether risk allocation for unauthorized transactions should be the same for credit cards, debit cards, and checks. This article focuses on

\footnote{155}{Id.}
\footnote{156}{Mann, \textit{supra} note 17, at 693.}
\footnote{157}{Id. at 694.}
\footnote{158}{Id.}
\footnote{159}{Id.}
\footnote{160}{Id.}
the equivalence of systems that allow for electronic funds transfers and the fact that errors may result. At the same time, harmonizing error resolution for funds transfer and debit cards is feasible given that the current procedures for credit and debit are similar but not identical.

CONCLUSION

In conclusion, there are various factors that indicate that a common error resolution procedure for retail payment systems would be beneficial—including market failure, creating an incentive with respect to loss prevention, and using loss allocation to make procedures more efficient. In the absence of uniformity, what can be done about error resolution in sectors that fall outside of the federal payments regulatory structure? As I have noted in a previous essay, the use of licensing regimes in the form of safety and soundness licensing for prepaid card issuers and payment intermediaries may serve to enforce some mandatory error resolution standards.161 State regulators could require entities such as PayPal or non-bank issuers of prepaid cards to maintain adequate error resolution procedures as part of a larger safety and soundness regime. Some commentators remain skeptical of light touch regulation at the state level. State regulators, however, could look to existing industry standards, which often mimic Regulation E processes and create a safe harbor for entities that comply with Regulation E or some other standard that is accepted by the industry.

Mann has noted that the Uniform Money Services Act (broadened to cover EBPP) might foster a useful path for the time being.162 He does not, however, address the problem of piecemeal state regulation. Co-regulation may be a useful solution that ultimately leads to greater uniformity in error resolution among payment systems.

162. Mann, supra note 17, at 705–06.
RUNAWAY BANDWAGON

HOW THE GOVERNMENT’S PUSH FOR DIRECT DEPOSIT OF SOCIAL SECURITY EXPOSES SENIORS TO PREDATORY BANK LOANS

July 2010
ABOUT THE AUTHORS

Leah A. Plunkett is a staff attorney at NCLC, where her areas of focus include predatory small dollar loans. Before coming to NCLC, Leah clerked in the United States District Court for the District of Maryland and established the Youth Law Project at New Hampshire Legal Assistance. Leah received her undergraduate and law degrees from Harvard University.

Margot Freeman Saunders is currently “of counsel” to NCLC, after serving as Managing Attorney of the Center’s Washington office from 1991 to 2005. Margot has testified before Congress on dozens of occasions regarding a wide range of consumer law matters, including predatory lending, payments law, electronic commerce, and other financial credit issues. She is a co-author of NCLC’s Consumer Banking and Payments Law and a contributor to numerous other manuals. Margot currently regularly serves as an expert witness in consumer credit cases, providing opinions on predatory lending, electronic benefits, servicing, and credit math issues. Prior to joining NCLC she was the consumer law specialist for North Carolina Legal Services. In 1991, Margot was the second recipient of the Vern Countryman Award. She is a graduate of Brandeis University and the University of North Carolina School of Law.

ACKNOWLEDGMENTS

Rick Jurgens, an investigative reporter and advocate at NCLC, contributed research and editorial content.

We would also like to thank Carolyn Carter of NCLC for her valuable guidance, feedback, and editorial review; Lauren Saunders of NCLC for sharing her expertise; Ana Lucia Hurtado and Tamar Malloy of NCLC for their editorial assistance; and Julie Gallagher for designing and formatting the report and its accompanying graphics and tables.

This report was funded in part by the Retirement Research Foundation. NCLC thanks the Foundation for its support. However, the findings and conclusions presented are those of the authors alone and do not necessarily reflect the views or position of the Foundation.

ABOUT THE NATIONAL CONSUMER LAW CENTER

The National Consumer Law Center®, a nonprofit corporation founded in 1969, assists consumers, advocates, and public policy makers nationwide on consumer law issues. NCLC works toward the goal of consumer justice and fair treatment, particularly for those whose poverty renders them powerless to demand accountability from the economic marketplace. NCLC has provided model language and testimony on numerous consumer law issues before federal and state policy makers. NCLC publishes an 18-volume series of treatises on consumer law, and a number of publications for consumers.
In 1996, when the federal government initiated efforts to shift recipients of federal payments to direct deposit, it had good intentions: to save the government billions of dollars in check processing costs, spare millions of trees from being cut down to make paper checks and envelopes, and deliver federal payments to beneficiaries more safely and efficiently.¹

Unfortunately, this 14-year drive has had unintended and devastatingly expensive consequences for some seniors. Large numbers of elderly, previously unbanked recipients of federal benefits became bank customers in order to receive direct deposit of Social Security benefits. That exposed these seniors’ funds to a new financial peril: fee-based overdraft protection. By the early 2000s, overdraft protection was a huge source of profit for banks.² Seniors and other recipients of Social Security are now key customers for these exorbitantly expensive programs.³

¹ 31 U.S.C. § 3332(f), (i)(2).

Now in 2010, the federal government is stepping up its push to shift the remaining 2.1 million Social Security recipients and 1.8 million Supplemental Security Income (“SSI”) recipients⁴ who still receive paper checks to electronic deposit. However, absent significant changes to proposed Treasury Department regulations, this renewed push is likely to inflict more financial harm on low-income seniors and other benefits recipients.

This new threat is even greater as new federal regulations take effect that will restrict banks’ ability to generate revenue from fee-based overdraft loan programs. Anxious to fill the projected void in their profits,⁵ banks are likely to turn to another expensive product that generates revenue from low-income, elderly, and other vulnerable customers: bank payday loans.⁶

Banks do not put the onerous “payday” label on these products. Instead, they are marketed as “account advances” or with similar

⁵ See, e.g., Fair Isaac Corp. (FICO), Insights: White Papers, Opting In or Out: Protecting Revenue Under Overdraft Reform 3 (2009), available at http://www.fico.com/en/FIResourcesLibrary/Insights_Opting_In_or_Out_2578WP.pdf (advising banks that they “can expect a significant financial impact to their income statement through changes in non-interest income” thus “new product development” is necessary).
innocuous labels. But bank “account advance” products amount to payday loans in all but name: cash loans to holders of bank accounts that receive direct deposits of benefits or other income.

Like fee-based overdraft, these “account advance” or “bank payday loan” products hit borrowers with astronomical fees or interest rates, offer nearly instant access, and require quick repayment. Despite the extraordinary expense of these loans to borrowers, they pose little or no risk to the banks. This lack of risk stems from a key component of these products: they give banks direct access to borrowers’ accounts, so if the borrower does not repay the loan within the (generally) 35-day time limit, the bank simply reaches into the borrower’s bank account and takes the money.

As a result, even after the much-heralded restrictions on overdraft lending take effect, banks will still provide high-cost, short-term loans to seniors and other vulnerable customers.

The number of seniors eligible for the bank payday loans through bank accounts and prepaid debit cards will almost certainly increase within the next several years as the federal government increases the pressure to move all federal beneficiaries to direct deposit. The Treasury Department has proposed a rule that would make it almost impossible for seniors to opt out of direct deposit and receive paper checks, thereby propelling more seniors into bank accounts. A second proposed rule would allow Social Security benefits to be deposited onto prepaid debit cards that operate as substitutes for bank accounts. Some of those cards include payday loan features.

Ironically, even as the Treasury Department’s push to eliminate paper checks drives seniors into the arms of high-cost lenders, Treasury has also been working hard to protect those same seniors from garnishments issued by judgment creditors.

---

7 Traditional payday loans are short-term high-cost loans secured by post-dated checks or agreements to debit electronically borrowers’ bank accounts. See generally Nat’l Consumer Law Ctr., The Cost of Credit § 7.5.5 (4th ed. 2009).

8 This report refers to this category of products as “bank payday loans”—except when referring to specific products, in which case the bank’s own label is used—to connote their similarities with payday loans made by non-bank storefront and internet lenders.


10 This report refers to the universe of reloadable electronic vehicles into which recipients can deposit their benefits with the shorthand “prepaid debit cards” to distinguish them from debit cards tied to bank checking accounts.


12 Under the terms of the proposed rule issued May 14, 2010, federal payments will be required to be either directly deposited into a bank account owned by the recipient, deposited onto the government-sponsored Direct Express card, or deposited onto other prepaid debit cards that meet certain criteria. None of the criteria will preclude the use of prepaid debit cards which are tied to bank payday loan products. See Federal Government Participation in the Automated Clearing House, 75 Fed. Reg. 27239 (proposed May 14, 2010) (to be codified at 31 C.F.R. pt. 210). Currently, both MetaBank and Urban Trust Bank offer a prepaid card that is available at check cashing and other outlets and appears to include a payday loan feature.

13 As Social Security and other government benefits are necessary for recipients to maintain a basic level of subsistence, federal law prohibits these benefits from seizure by creditors. 42 U.S.C. § 407 (Social Security); 42 U.S.C. § 1383(d)(1) (SSI); 38 U.S.C. § 5301(a) (VA benefits).
of 2010, the Treasury Department, along with several other federal agencies, proposed a well-considered and thorough rule requiring banks to protect direct-deposited federal benefits from seizure to satisfy garnishment orders by judgment creditors.\textsuperscript{14}

The purpose of this report is to highlight the continuing—and increasing—threat to the recipients of federal benefits from high-cost, short-term loan products issued \textit{by the institutions which are the repositories for those federal benefits}. The report examines the illogic of the federal agencies’ recognition, on the one hand, of the need to protect those benefits from third-party judgment creditors, while on the other hand, failing to propose any meaningful protections against the pernicious loan products offered by banks to their customers with checking accounts or prepaid cards. The report concludes that the federal government must take responsibility for ensuring that the bank accounts and prepaid debit cards into which Social Security and other federal benefits are deposited will not bleed seniors and other recipients of vital subsistence resources.


RUNAWAY BANDWAGON
HOW THE GOVERNMENT’S PUSH FOR DIRECT DEPOSIT OF SOCIAL SECURITY EXPOSES SENIORS TO PREDATORY BANK LOANS

TABLE OF CONTENTS

I. Social Security Benefits Save Seniors from Poverty. 5
II. Social Security Benefits Are Going to Pay for High-Cost, Short-Term Loans. 6
III. The Questionable Legality of Bank and Prepaid Debit Payday Loans 18
IV. An Illustration of the Exorbitant Cost of Bank Payday Loans 21
V. The Direct Deposit Push: Past and Present 22
VI. Recommendations for Keeping Federal Benefits Safe 25
   Conclusion 26

Appendices
A. Disclosed APRs Hid Costliness of Wells Fargo Direct Deposit Advances 27
B. Fees and More Fees 28
C. An Account on the Edge 30
I. SOCIAL SECURITY BENEFITS SAVE SENIORS FROM POVERTY.

All too many Social Security recipients experience life as a struggle to survive. They face relentless increases in the costs of essentials such as medical care and housing. Social Security, a social insurance program that seniors have paid into during their working lives, constitutes a critical lifeline for many. “Nearly half of all seniors would be living below the poverty line were it not for Social Security.”

In 2009, the Social Security Administration paid more than $680 billion in retirement, disability, and supplemental income benefits to 56 million recipients. As of December 2009, about 37 million of those recipients were aged 65 or older.

However, researchers have found that even with Social Security income “close to four of five senior households [still] do not have sufficient economic security to sustain them through their lives.”

Most government benefits payments are relatively small. The average monthly Social Security retirement payment as of December 2009 was only $1,164.30. Yet many recipients—especially those with low incomes, few savings, and little or no coverage by private pensions—depend upon those benefits to buy food, shelter, medicine, and other items necessary for survival. In 2008, Social Security benefits accounted for more than 88% of all income received by the poorest 40% of the senior population.

To preserve federal benefits for their intended recipients, Congress provided that the benefits cannot be seized to pay debts, as such seizures would result in the loss of subsistence funds. The Social Security Act says:

The right of any person to any future payment under this subchapter shall not be transferable or assignable, at law or in equity, and

None of the moneys paid or payable

---

1 See, e.g., Deanne Loonin & Elizabeth Renuart, The Life and Debt Cycle: The Growing Debt Burdens of Older Consumers and Related Policy Recommendations, 44 Harv. J. on Legis. 167, 171 (Winter 2007); West Virginia Ctr. on Budget & Pol’y et al., Long Term Care Partnership, and Wider Opportunities for Women, Elders Living on the Edge: When Basic Needs Exceed Income in West Virginia 1, 1 (2010), available at http://www.wvpolicy.org/downloads/WV_Elder_Policy_Brief060210.pdf (explaining that “today’s elders are pressured by increasing housing, health care, food and utility expenses while the value of their assets and their incomes are eroded by weaknesses within the economy”).


or rights existing under this subchapter shall be subject to execution, levy, attachment, garnishment, or other legal process, or to the operation of any bankruptcy or insolvency law.\textsuperscript{8}

The statutes governing the distribution of other federal benefits, such as VA benefits, similarly articulate that these funds are to be free from attachment or garnishment or other legal process.\textsuperscript{9}

\textsuperscript{8}42 U.S.C. § 407(a) (emphasis added).
\textsuperscript{9}42 U.S.C. § 407(a). The protections are similar in the other federal statutes governing federal benefits:

\textit{VA benefits:} Payments of benefits due or to become due under any law administered by the Secretary shall not be assignable except to the extent specifically authorized by law, and such payments made to, or on account of, a beneficiary shall be exempt from taxation, shall be exempt from the claim of creditors, and shall not be liable to attachment, levy, or seizure by or under any legal or equitable process whatever, either before or after receipt by the beneficiary. 38 U.S.C. § 301(a)(1).

\textit{Railroad Retirement benefits:} Except as provided in subsection (b) of this section and the Internal Revenue Code of 1986 [26 U.S.C.A. § 1 et seq.], notwithstanding any other law of the United States, or of any State, territory, or the District of Columbia, no annuity or supplemental annuity shall be assignable or be subject to any tax or to garnishment, attachment, or other legal process under any circumstances whatsoever, nor shall the payment thereof be anticipated. 45 U.S.C. § 231m.

\textit{Federal Retirement program benefits:} An amount payable under subchapter II, IV, or V of this chapter is not assignable, either in law or equity, except under the provisions of section 8465 or 8467, or subject to execution, levy, attachment, garnishment or other legal process, except as otherwise may be provided by Federal laws. 5 U.S.C. § 8470.

II. SOCIAL SECURITY BENEFITS ARE GOING TO PAY FOR HIGH-COST, SHORT-TERM LOANS.

The crystal-clear policy articulated in the federal laws establishing the benefit programs protects these funds from being seized to pay debts involuntarily through garnishment and attachment. Yet banks, when extending credit through payday loan programs, claim the right to seize these protected funds to repay the payday loans.

Banks claim that the prohibitions against seizure—through garnishment and attachment, which apply to debts owed to third parties—do not apply when the bank is also the creditor. As a result, when banks make payday loans, Social Security and other beneficiaries are vulnerable to the same dangers from seized benefits as result from attachment and garnishment. Instead of functioning as financial safe havens for these essential benefits, banks make high-cost, short-term loans and then take the loan repayment and exorbitant fees directly out of the supposedly protected Social Security benefits—a step that federal law appears to prohibit.\textsuperscript{10}

There are three ways in which banks threaten Social Security and other benefits:

1. The well-known, declining, but still thriving overdraft protection plans;

\textsuperscript{10}There is a legal distinction between the seizure of benefits to satisfy a garnishment or attachment order of a third-party creditor and the seizure of benefits by the repository of those benefits. The latter situation requires the operation of the bank’s use of its common law and contractual power of set-off. The legality of a bank’s use of the power of set-off is examined more fully in section III \textit{infra}. 
2. The less well-known but very costly bank payday loan programs;

3. The expansion of bank payday loans to holders of prepaid debit cards.

All are threats from FDIC-insured, federally regulated banks and savings and loan associations. These high-cost, short-term loan products—fee-based overdraft programs and bank payday loans—share nearly identical basic characteristics with the predatory payday loans offered by the non-bank payday lenders that are ubiquitous in storefronts in many states and on the Internet.

1. How Fee-Based Overdraft Works

Among bank products and services that pose hidden perils to customers, the most well-known are fee-based overdraft programs. Under these programs, banks cover the amount of a check, point of sale (POS) debit card purchase, or ATM withdrawal when there are insufficient funds in the customer’s bank account. Banks charge the customer a fee, typically around $35, each time they cover an overdraft. Some banks also charge a daily fee if a customer’s account balance remains negative. Banks then take some or all of the customer’s next deposit to repay themselves the amount covered, the one-time fee, and the daily fee (if applicable).

A typical overdraft product carries an Annual Percentage Rate (“APR”) of 1,820%. The customer is unlikely to realize the true cost of a fee-based overdraft loan, as banks take advantage of loopholes in the Truth in Lending Act to avoid APR disclosures.

Fee-based overdraft loans have much in common with standard payday loans:

- Both require the customer to give the lender direct access to a bank account for credit to be extended. Payday lenders obtain this access by having the borrower write a post-dated check or sign an electronic debit agreement, while banks simply deduct the loan amounts.

13 References to the APR in this report are to the APR as calculated according to the federal Truth in Lending Act. The Truth in Lending Act APR is a uniform way to determine the true cost of a loan. It is expressed as a percentage and includes most of the fees and charges associated with the loan, as well as the interest to be earned over the term. See 15 U.S.C. §§ 1605, 1606. The APR has been the credit cost yardstick in this country for forty years and aims to provide an apples-to-apples comparison of the cost when consumers shop. See Elizabeth Renuart & Diane Thompson, The Truth, The Whole Truth, and Nothing but the Truth: Fulfilling the Promise of Truth in Lending, 25 Yale J. on Reg. 181, 186–91 (2008); Matthew A. Edwards, Empirical and Behavioral Critiques of Mandatory Disclosure: Socio-Economics and the Quest for Truth in Lending, 14 Cornell J.L. & Pub. Pol’y 199, 211–15 (2005).


15 See Nat’l Consumer Law Ctr., The Cost of Credit § 7.5.6.2 (4th ed. 2009).
Another difference is that payday loans require the customer to apply affirmatively, either at a brick and mortar store or over the Internet.20 Banks, however, have historically enrolled customers automatically in fee-based overdraft programs.21 This meant that some customers were unaware that they were being given a loan until the fees showed up on their account statements. Under new federal regulations that take effect during the summer of 2010,22 bank customers must affirmatively opt in to be covered by fee-based overdraft protection plans for ATM or one-time debit card transactions that put an account in the red.23 However, the new regulations still allow banks to make overdraft loans even when the customer has not specifically agreed to the program, for example, when the customer incurs an overdraft by writing a paper check.24

Overdraft fees have represented a huge source of revenue to banks. In 2008, banks and credit unions received almost $24 billion in fee-based overdraft revenue—a 35% increase from two years earlier.25 When non-

20 See Nat’l Consumer Law Ctr., The Cost of Credit §§ 7.5.5.2, 7.5.5.4 (4th ed. 2009).
Making the conservative assumption that overdraft expenses of recipients came equally from their Social Security and other income, at least $700 million of Social Security benefits has gone to pay overdraft fees each year. This estimate is conservative because direct-deposited Social Security funds are more likely than non-direct deposited sources of income to go toward overdraft fees because they are, by definition, going into the consumer’s bank account. Banks can then help themselves to these funds immediately upon their addition to the account. By contrast, consumers can choose whether to put non-direct deposited income into their accounts or keep it elsewhere, thus making it less vulnerable to going to pay overdraft fees.

2. How Bank Payday Loans (a/k/a “Account Advance” Products) Work

For at least fifteen years, some banks have offered other high-cost, short-term loan products, generally referred to as “account advances,” that closely resemble payday loans. In recent months, bank payday loans made to bank account holders and to holders of prepaid debit cards (described in more detail below) have become increasingly prominent in the marketplace. Banks offering these products include large institutions like Wells Fargo as well as smaller institutions, such as Guaranty Bank. The chart below sets forth an overview of the key terms of bank payday loan products.

(Text continues on page 16.)

---

sufficient fund (NSF) fees for bounced checks were included along with overdraft fees, one analysis estimated that the total revenue to banks and credit unions in 2008 was in excess of $34.7 billion.26 According to a 2009 report, consumers “spend about the same amount on overdraft fees as they do on fresh vegetables every year, and only a little less than they do on fresh fruit.”27

Many overdraft fees are paid out of Social Security funds. The Center for Responsible Lending estimates that adults aged 55 and over pay $6.2 billion a year in overdraft fees.28 Within this group, those receiving at least half of their income from Social Security (of all types, but not including Supplemental Security Income) pay almost $1.4 billion each year in overdraft fees.29

---

## Bank Payday Loan Products

Six banks offer high-cost loans to customers with checking accounts or prepaid debit cards.

<table>
<thead>
<tr>
<th>Bank</th>
<th>Product Name</th>
<th>Cost and Fee Structure</th>
<th>Minimum Loan</th>
<th>Maximum Loan</th>
<th>Disclosed APR*</th>
<th>Actual APR**</th>
<th>Minimum Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fifth Third Bank, Cincinnati, OH</td>
<td>Early Access</td>
<td>Transaction fee of $1 per every $10 borrowed (10% of amount of cash advance). No late payment or over-the-credit limit penalties.</td>
<td>$1</td>
<td>The lesser of $500 or half of combined monthly direct deposits of $100 or more, rounded up to next multiple of $20. Calculation based on 3 month average.</td>
<td>120%</td>
<td>261%</td>
<td>None.</td>
</tr>
</tbody>
</table>

| U. S. Bank, Minneapolis, MN | Checking Account Advance | $2 per $20 borrowed (10% of amount of cash advance). | $20, or amount (rounded to nearest $20) required to erase negative balance in account. | The lesser of $500 or half of the total direct deposits listed on most recent checking account statement rounded up to the next $20. | 120% | 261% | None. |

<p>| Wells Fargo Bank, San Francisco, CA | Direct Deposit Advance | $2 for each $20 borrowed (10% of amount of cash advance). $35 late fee if not repaid by specified due date. | $20 | One half of &quot;monthly qualified deposit&quot; income rounded up to the nearest $100, but no more than $500. Also, no more than $300 in first month of eligibility or after lapse of qualified deposit income. Maximum credit reduced by $100 after 12 consecutive months of advances, and by an additional $100 each month of additional advances. | 120% | 261% | Until next direct deposit. |</p>
<table>
<thead>
<tr>
<th>MAXIMUM DURATION</th>
<th>ELECTRONIC REPAYMENT TERMS AND OPTIONS</th>
<th>NON-ELECTRONIC REPAYMENT OPTIONS</th>
<th>DIRECT DEPOSIT REQUIREMENT</th>
<th>OTHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>35 days</td>
<td>Repayment is automatically deducted from next direct deposit of $100 or more. Will not be deducted from other deposits. If next direct deposit does not repay in full, whole deposit will be seized. If balance is not paid in full by 35th day from direct deposits, balance will be deducted from account, even if doing so overdraws account and leads to overdraft fees.</td>
<td>Manual repayment at any time.</td>
<td>Must have received direct deposit of at least $100 in two consecutive statement cycles, including one no more than 35 days prior to account advance, to a checking account in good standing held by an individual adult, open for at least six months and not subject to legal process or being charged off.</td>
<td>No application required. Offer limited to eight states: OH, KY, TN, MI, IL, FL, IN, MO. May lose eligibility in certain situations, including: ineligible for 30 days after borrowing up to amounts of credit limit in 6 consecutive months; ineligible for 60 days if account overdrawn for 10 or more consecutive days or 20 or more times in the previous 2 months.</td>
</tr>
<tr>
<td>35 days, except under &quot;Payment Plan.&quot;</td>
<td>Repayment is automatically deducted from next direct deposit of $100 or more. Will not be deducted from other deposits. If next direct deposit does not repay in full, whole deposit will be seized. If balance is not paid in full by 35th day from direct deposits, balance will be deducted from account, even if doing so overdraws account and leads to overdraft fees.</td>
<td>Manual repayment at any time.</td>
<td>Must have received one direct deposit of at least $100 in two consecutive statement cycles, including fees.</td>
<td>No application necessary if eligibility criteria are met. May lose eligibility in certain situations, including: eligibility suspended for 90 days after getting advances in 9 consecutive statement cycles; until account has a zero or positive balance if checking account overdrawn for 5 consecutive business days; until overdrafts are reduced if checking account overdrawn &quot;an excessive number of times.&quot; Account advance agreement terminates automatically after failure to take advance for 12 consecutive statement cycles. Social Security is listed as an example of a direct deposit.</td>
</tr>
<tr>
<td>35 days</td>
<td>Repayment by mail in some states after payment of one-time set up fee of $100, subject to $35 late fee if not repaid by due date. $100 fee will be charged again if borrower moves from payment by mail back to automatic repayment then back to payment by mail again. Payment by mail option also allows for payments to be made by phone.</td>
<td>Checking account must be held by an individual adult, be in good standing, and not subject to legal process. Account must receive at least one recurring electronic direct deposit of $100 or more every 35 days from an employer or outside agency, which could include a recurring payroll or other benefit related income or a special one time, non-repetitive electronic deposit. Account must have completed a full statement cycle with a qualified deposit to be eligible for an advance. An interruption in qualified deposit income will make account ineligible for the service.</td>
<td>Qualify for advance when direct deposit made into checking account in good standing. Advances suspended while in Payment Plan. May lose eligibility in certain situations, including: no access for 6 days if account overdrawn for 7 consecutive days; eligibility suspended for 90 days if overdraft created by automatic repayment is not paid in full within 8 days; eligibility permanently discontinued if there is fraud or a bankruptcy petition. Binding arbitration with American Arbitration Association. ATM access suspended 2/22/10. Credit limit may be reduced down to $0 if advances have been taken for 12 or more consecutive statement periods, but will be re-instated after no advances for one statement period.</td>
<td></td>
</tr>
</tbody>
</table>
### Bank Payday Loan Products (continued)

<table>
<thead>
<tr>
<th>BANK</th>
<th>PRODUCT NAME</th>
<th>COST AND FEE STRUCTURE</th>
<th>MINIMUM LOAN</th>
<th>MAXIMUM LOAN</th>
<th>DISCLOSED APR*</th>
<th>ACTUAL APR**</th>
<th>MINIMUM DURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urban Trust Bank, Lake Mary, FL</td>
<td>Elastic</td>
<td>$2.50 transaction fee for each $20 borrowed (12.5% of amount borrowed). Also, $2.50 per $20 extension fee plus pay off of at least 10% of most recent Elastic Cash draw from line of credit for Elastic Pay repayment option.</td>
<td>$0</td>
<td>Up to $500 at determination of Urban Trust Bank.</td>
<td>Not disclosed.</td>
<td>326%</td>
<td>None; can repay in full at any time.</td>
</tr>
<tr>
<td>MetaBank, Storm Lake, IA</td>
<td>iAdvance</td>
<td>$2.50 transaction fee for each $20 borrowed (12.5% of amount borrowed). No fees for late or early payments.</td>
<td>$20</td>
<td>Credit limit determined by bank.</td>
<td>150%</td>
<td>326%</td>
<td>Until next direct deposit.</td>
</tr>
</tbody>
</table>
### Bank Payday Loan Products (continued)

<table>
<thead>
<tr>
<th>Maximum Duration</th>
<th>Electronic Repayment Terms and Options</th>
<th>Non-Electronic Repayment Options</th>
<th>Direct Deposit Requirement</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>After 10 consecutive months with an outstanding balance, borrower is ineligible for additional draws of Elastic Cash until balance reaches $0.</td>
<td>Borrower may schedule electronic payments. If borrower does not make minimum payment by due date, a payment of at least 10% of outstanding Elastic Cash balance from most recent draw is automatically deducted from transaction account (called “Elastic Pay” amount). Note that there are fees associated with Elastic Pay option. Any amount electronically transferred directly into transaction account can be used for this automatic repayment.</td>
<td>Borrower may make payment by mail. But if borrower does not make minimum payment by due date, same automatic deduction applies as it does for electronic repayment.</td>
<td>Must be at least 21 and have a regular source of income or benefits deposited to a transaction account: a bank checking account (not necessarily with Urban Trust Bank), ElasticCard (from Urban Trust Bank), or other prepaid debit card issued by provider under agreement with Urban Trust Bank. Checking account, ElasticCard, or other prepaid debit card must not be frozen or subject to legal process.</td>
<td>Borrowers must meet Urban Trust Bank’s underwriting standards and complete application online. Borrowers will find out “right away” if they are approved. Elastic Credit terminates after 12 consecutive months without use. Forced arbitration by American Arbitration Association or JAMS, The Resolution Experts, but limited in California. Elastic Card is a prepaid Visa debit card; Cardholder Agreement says that card can be loaded via direct deposit by government agency. Deposits onto Elastic Card are FDIC insured. Elastic Credit application asks about Social Security/Disability and Retirement/Pension income; states that you don’t have to be employed to qualify for this line of credit but must have regular income.</td>
</tr>
<tr>
<td>35 days</td>
<td>Repayment is automatically deducted from next direct deposit from any source to prepaid card. If next direct deposit doesn’t repay in full, bank will automatically deduct amount owed from any funds on prepaid card, including future deposits, until repayment made in full.</td>
<td>Must be age 18 or older and have a prepaid card that receives direct deposit of wages, other income, or benefits at intervals of no more than 35 days in qualifying dollar amounts. Prepaid card must be eligible for iAdvance (AccountNow, NetSpend Visa Prepaid Card, Jackson Hewitt ipower Visa Prepaid Card, MiCash Prepaid MasterCard, MoneyGram Visa Prepaid Card, as well as some payroll cards). These prepaid debit cards are issued by MetaBank under licenses from the Visa or MasterCard networks; some of these cards are co-branded with other financial services companies. Eligible for advance after at least one such direct deposit has been made.</td>
<td>Application required; borrowers can then have “money available to you in seconds.” Up to 10 transactions per day. Note that AccountNow and NetSpend direct deposit forms instruct borrower to give the form to her employer or benefits provider, while the Jackson Hewitt form just mentions payroll administrator.</td>
<td></td>
</tr>
</tbody>
</table>

---

**Note:**

1. **National Consumer Law Center**
2. **The Debt Machine**
3. **Page 13**
### Bank Payday Loan Products (continued)

<table>
<thead>
<tr>
<th>Bank</th>
<th>Product Name</th>
<th>Cost and Fee Structure</th>
<th>Minimum Loan</th>
<th>Maximum Loan</th>
<th>Disclosed APR*</th>
<th>Actual APR**</th>
<th>Minimum Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guaranty Bank, Milwaukee, WI</td>
<td>Easy Advance</td>
<td>$25 non-refundable application fee for each advance sought, regardless of whether advance is approved. Fee deducted from checking account as soon as application processed.</td>
<td>$200</td>
<td>With direct deposit, the lesser of $400 or half of the average direct deposits to account in each of the last 3 months; without direct deposit, $200.</td>
<td>Approximately 230% on a $360 advance if the entire balance of the advance was outstanding for 11 days, but notes that application fee is not technically a finance charge under the federal Truth In Lending Act.</td>
<td>217%</td>
<td>Until next direct deposit or any deposit of $100 more (if borrower is not a qualified direct deposit customer).</td>
</tr>
</tbody>
</table>

* Disclosed APRs for Fifth Third Bank, US Bank and MetaBank appear to be based on an advance with a 30-day duration using a 360-day year.

** Actual APR is computed based on a borrower obtaining a $300 advance with a 14-day duration, comparable to a closed-end loan of the same duration using a 365-day year; for Guaranty Bank, the actual APR is computed based on a borrower obtaining a $325 advance (netting $300 in cash after the upfront application fee) with a 14-day duration, comparable to a closed-end loan of the same duration using a 365-day year.

---


### Bank Payday Loan Products (continued)

<table>
<thead>
<tr>
<th>Maximum Duration</th>
<th>Electronic Repayment Terms and Options</th>
<th>Non-Electronic Repayment Options</th>
<th>Direct Deposit Requirement</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>35 days</td>
<td>Repayment is automatically deducted from next direct deposit of $100 or more or any deposit of $100 or more (if borrower is not a qualified direct deposit customer). If next direct or other deposit does not repay in full, whole deposit will be seized. If balance is not paid in full by 35th day, the balance will be deducted from the account, even if doing so overdraws account and leads to overdraft fees.</td>
<td>Not required. Considered to have direct deposit if in each of the previous 3 months account received a direct deposit of $75 or more from employer, a governmental agency or other payor. Direct deposits may include both recurring and one-time deposits, such as a tax refund. Must be age 18 or above. Must have checking account (personal, individual, or joint) in good standing open for 120 days that received at least $500 in deposits (of at least $75 each) in each of the last three months. Must not be in bankruptcy and account must not be subject to legal process.</td>
<td>&quot;Approvals are instant with no paper work [sic] to complete.&quot; May lose eligibility in certain situations, including: access suspended until positive balance is restored and maintained for at least six days if account is overdrawn for 7 consecutive business days. After 12 consecutive advances, not eligible for advance for 35 days after 12th advance repaid in full. Forced arbitration of disputes.</td>
<td></td>
</tr>
</tbody>
</table>
Account advance products look just like payday loans, except they are offered directly by banks. Account advance products typically work as follows.\textsuperscript{30} First, the customer asks her or his bank for an “advance” of funds, which the bank schedules to deposit into the customer’s account. Provided the customer meets minimal eligibility criteria, such as direct deposits of a certain frequency and amount, the bank automatically advances the funds. The bank then repays itself in full for the advance plus the fee by taking some or all of the customer’s next deposit. If this deposit is insufficient to repay the bank in full, the bank keeps taking subsequent deposits.\textsuperscript{31} If deposits within 35 days do not fully cover the loan plus the fees incurred, the bank simply overdraws the customer’s account to repay itself. The bank’s withdrawals often leave the account with insufficient funds to cover checks the consumer has written, leading to a cascade of overdraft fees.

“Advance” amounts are usually capped at $500 and cost at least $10 per $100 loaned. While banks do disclose sample account advance APRs to consumers, the disclosed rate is generally 120%. However, the actual cost incurred by the customer depends on the length of time the loan is outstanding: the shorter the repayment time, the higher the APR.\textsuperscript{32} For example, under the terms of Wells Fargo’s Direct Deposit Advance product, the actual APR can be as high as 1,825%, as demonstrated by an analysis of the account of one borrower who took out an account advance with a two-day duration (see Appendix B).

The new limitations on overdrafts, which will require affirmative consumer opt-in for banks’ overdraft loan programs, will likely reduce banks’ overdraft fee revenues, perhaps by 27% to 34%.\textsuperscript{33} Banks are likely to push customers toward bank account advance loans to replace this lost revenue,\textsuperscript{34} making these high-cost, predatory loans a growing threat to seniors. Because most seniors receiving Social Security benefits do so via direct deposit,
they will likely be a key target for increased marketing of bank payday loan products. Indeed, payday lenders have long welcomed the opportunity to make loans to Social Security and other benefit recipients because these recipients have regular sources of income that can be tapped for repayment. The activities of payday lenders who solicit Social Security beneficiaries to take out high-interest loans have already been noticed by the Social Security Administration.

Many low- and moderate-income seniors are now enduring a recession which has exacerbated long-standing financial pressures that result from rising living costs, diminished savings, and insecure incomes. To survive, many are forced to borrow money to meet essential expenses, making them more vulnerable to the marketers of bank payday loans.

3. How Bank Payday Loans to Prepaid Debit Card Holders Work

At least two banks, Urban Trust and MetaBank, offer expensive, payday loan like account advances through prepaid debit cards issued by them, sometimes in conjunction with other financial services providers.

Prepaid debit cards are used by many recipients of Social Security and other federal benefits. Some of those recipients are not permitted bank accounts because of past troubles with banks, while others choose not to use banks for one reason or another.

Payments to many of these unbanked recipients of Social Security and other benefits are distributed by direct deposits through alternative financial providers such as check

---


37 See, e.g., Deanne Loonin & Elizabeth Renuart, The Life and Debt Cycle: The Growing Debt Burdens of Older Consumers and Related Policy Recommendations, 44 HARV. J. ON LEGIS. 167, 170-73 (2007) (discussing the squeeze on seniors from decreasing resources and increasing living expenses); WEST VIRGINIA CENTER ON BUDGET & POLICY, LONG TERM CARE PARTNERSHIP, AND WIDER OPPORTUNITIES FOR WOMEN, ELDERS LIVING ON THE EDGE: WHEN BASIC NEEDS EXCEED INCOME IN WEST VIRGINIA 1, 1 (2010), available at http://www.wvpolicy.org/downloads/WV_Elder_Policy_Brief060210.pdf (explaining that “today’s elders are pressured by increasing housing, health care, food and utility expenses while the value of their assets and their incomes are eroded by weaknesses within the economy”).

38 See Deanne Loonin & Elizabeth Renuart, The Life and Debt Cycle: The Growing Debt Burdens of Older Consumers and Related Policy Recommendations, 44 HARV. J. ON LEGIS. 167, 170-73 (2007) (explaining that seniors are “going into debt and filing for bankruptcy in record numbers” and that the debt is often “unaffordable”).
The advances made by Urban Trust and MetaBank through prepaid debit cards are essentially bank payday loan products, although the mechanics are slightly different. Instead of having a bank account into which benefits or other sources of income are deposited, the borrowers’ funds appear to be deposited first into pooled accounts and then onto the debit card. Account advance features, such as MetaBank’s iAdvance line of credit or Urban Trust’s Elastic, transform prepaid debit cards into credit instruments. As with payday loans tied to individuals’ bank accounts, the accounts must meet certain criteria, including regular direct deposits, and the bank will typically repay itself for the advance plus the fee from subsequent direct deposits.

III. THE QUESTIONABLE LEGALITY OF BANK AND PREPAID DEBIT PAYDAY LOANS

The legality of these bank and prepaid debit card payday loans is highly questionable in several respects, especially when protected Social Security or other federal benefits are used to repay the loans.

1. Section 207 of the Social Security Act

The first analysis is under Section 207 of the Social Security Act and similar protections in other federal statutes which prohibit garnishment, attachment, or other legal process against Social Security or other federal benefits.

---

39 According to a recent Inspector General’s report, which performed a “limited analysis” of the use of non-bank repositories, 35,705 individuals received their SSA payments through non-bank providers. These SSA payments, totaling approximately $25 million, were deposited into accounts held in the name of the provider in nine different banks, and then distributed the funds to the recipients. Office of the Inspector General, Social Security Admin., Old-Age, Survivors and Disability Insurance Benefit Payments Sent to Non-Bank Financial Service Providers, A-06-09-29090, at 5 (2010), available at http://www.ssa.gov/oig/ADOBEPDF/audittxt/A-06-09-29090.html.

40 The market includes a confusing variety of programs used by recipients to access their federal benefits when they do not have bank accounts. Some use private-label debit cards offered by non-banks; some use debit cards which can be used in MasterCard and Visa networks. Other prepaid debit cards are sold by merchants, payday lenders or check cashers, and licensed for use through the MasterCard or Visa networks. The cards are provided to recipients of federal benefits as an alternative means to receive the direct deposits. See generally Consumers Union, Prepaid Cards: Second-Tier Bank Account Substitutes (Aug. 2009), available at http://www.defendyourdollars.org/Prepaid%20WP.pdf (analyzing prepaid cards available for this purpose). Some programs are offered through check cashers or small loan companies that require recipients to physically go down to the provider and pick up their check and then pay to have their check cashed. These alternative non-bank distribution systems can be quite expensive for the recipients, who often must pay multiple fees just to access their money. For example, a recipient may be charged separately for all of the following: making each deposit, receiving a paper check in the amount of a benefits payment, cashing that check, and purchasing money orders or other payment products. See Office of the Inspector General, Social Security Admin., Old-Age, Survivors and Disability Insurance Benefit Payments Sent to Non-Bank Financial Service Providers, A-06-09-29090, at 6 (2010), available at http://www.ssa.gov/oig/ADOBEPDF/audittxt/A-06-09-29090.html.

benefits. Banks collect the debts for these loans by deducting the amount due from the borrower’s bank account, a procedure called “set-off.”

Numerous cases have held that it is illegal for banks to exercise their set-off right against federally exempt funds. Yet, ever since 2003, when the U.S. Supreme Court decided Washington State Dep’t of Health & Human Servs. v. Guardianship Estate of Keffeler, banks have argued that their use of set-off is explicitly excluded from the protections enumerated in section 207 of the Social Security Act.

The Supreme Court’s decision in Keffeler is in fact irrelevant to the issue of whether a bank can access the protected funds to repay debts owed to the bank. Keffeler did not address the authority of a bank to have preferential treatment over all the recipient’s other creditors. Keffeler arose from an entirely different situation. There, the Court upheld the State of Washington’s self-reimbursement for the maintenance of foster children in its care from the foster children’s Social Security benefits. The State was accessing the benefits lawfully by serving as the children’s representative payee, and the Court recognized the State’s right to fill this important role for its foster children. By contrast, the practice which we are concerned about involves banks taking exempt funds—without the explicit legal approval for doing so that exists for representative payees—for the banks’ sole benefit, to the clear detriment of recipients.

Moreover, cases both before and after Keffeler have specifically held that banks may not set off their own claims against exempt federal funds. Indeed, in a post-Keffeler reported decision concerning whether Section 207 prohibits a bank from taking exempt funds to pay a debt owed to it, a federal district court analyzed the case law and found that the pre-Keffeler prohibition against bank setoffs still applies. To support its rejection of bank set-offs against exempt funds, the federal district court quoted the Tenth Circuit:

We can see no reason why Congress would, on the one hand, choose to protect

---


44 Id. at 389-92.


Social Security beneficiaries from creditors who utilized the judicial system, a system that is built upon principles of fairness and protection of the rights of litigants, yet, on the other hand, leave such beneficiaries exposed to creditors who devised their own extra-judicial methods of collecting debts.47

2. Electronic Fund Transfer Act

The Electronic Fund Transfer Act (EFTA) prohibits creditors from requiring debtors to authorize electronic fund transfers to repay debts.48 Yet, in one way or another, all of the products that this report has reviewed essentially permit the bank-creditors unfettered access to the borrowers’ bank accounts. Even when the borrower is trying to repay the loan manually (by mail or in person) the product descriptions generally appear to provide no way for the borrower to stop the bank from seizing amounts still due at the end of the loan term (in most cases 35 days after the money was lent).

In a few products, the guidelines do appear to permit the borrower to close down the automatic payment option which permits the bank to seize the balance directly from the account. But this option is only available if 1) the borrower pays a significant fee to exercise this option, and 2) the fee is paid before incurring the debt. The product guidelines require that the loan will be repaid using the same terms in existence when the loan was made. The $100 Wells Fargo fee, 20% of the maximum credit limit, is so large that it is highly unlikely that most borrowers will choose to pay it. Moreover, there is no reason to believe that the bank would not still exercise what it generally believes to be its contractual set-off right to seize the funds if the loan was not repaid when due.

As a result, the requirements that existing credit be repaid using the debit method appear to mean that electronic fund transfers to repay the loans are indeed mandatory, and thus in violation of the EFTA.

3. Failure to determine ability to repay

Additionally, banks are prohibited from making loans without first determining the borrower’s ability to repay the loan. The regulations governing bank lending by national banks explicitly provide—

(b) Standards for loans. A national bank shall not make a consumer loan subject to this § 7.4008 based predominantly on the bank’s realization of the foreclosure or liquidation value of the borrower’s collateral, without regard to the borrower’s ability to repay, including, for example, the borrower’s current and expected income, current and expected cash flows, net worth, other relevant financial resources, current financial obligations, employment status, credit history, or other relevant factors.49

Needless to say, banks do not appear to analyze the affordability of these bank payday loans before making the loans. In fact, the typical bank payday loan is not affordable—it is made to a person who is already unable to meet current obligations and will be left in even more desperate straits by the payday loan. The only real core criterion for the loans is the receipt of a certain number of recurring payments.

47 Tom, 151 F.3d at 1292 (citing Crawford v. Gould, 56 F.3d 1162, 1166 (9th Cir. 1995)).


49 12 C.F.R. § 7.4008(b).
direct deposits at or above a set dollar amount into a bank account in good standing or onto a prepaid debit card.\textsuperscript{50}

The lending rules applicable to national banks are also applicable to state banks regulated by the FDIC.\textsuperscript{51} In 2007, the FDIC issued guidelines for the use of state bank charters for payday lending made by non-bank partners.\textsuperscript{52} Furthermore, \textit{most, if not all, of these banks’ programs appear to violate} the guidelines that govern whenever banks make small loans.\textsuperscript{53} These provisions require the bank to:\textsuperscript{54}

\begin{itemize}
  \item Collect fees that bear a direct relationship to origination costs and avoid charges such as annual fees, membership fees, advance fees, and prepayment penalties;
  \item Offer small-loan credit with APRs of no greater than 36%;
  \item Encourage principal reduction by structuring closed-end loans to provide for affordable and amortizing payments; open-end loans should require minimum payments that pay off principal;
  \item Avoid excessive renewals or the prolonged failure to reduce the outstanding balance; and
  \item Utilize sound underwriting that focuses on a borrower’s history with the institution and ability to repay within an acceptable timeframe, though for small loans, documenting the borrower’s ability to repay could be streamlined to include basic information, such as proof of recurring income.
\end{itemize}

IV. AN ILLUSTRATION OF THE EXORBITANT COST OF BANK PAYDAY LOANS

Use of high-cost, short-term loans can have devastating effects on consumers, trapping them in a cycle of repeat borrowing and constraining their ability to provide for their basic needs. Rather than help borrowers survive, these loans can push them closer to the financial brink.

Consider the story of Mr. B,\textsuperscript{55} who after using Wells Fargo’s Direct Deposit Advance program, found himself paying exorbitant interest rates and locked in a cycle of debt that aggravated rather than alleviated financial distress. A review of 39 consecutive monthly statements showed that Mr. B had taken out 24 Direct Deposit Advances, totaling $12,000. These account advance loans had an average duration of just over eight days, with the shortest running just two days and the longest twenty-one days. The finance charges for these short-term loans totaled $1,200, and their effective APRs ranged from 182% to 1,825%.

Ironically, even though account advance loans are marketed as a way of avoiding overdraft fees, Mr. B still ended up paying $676 in overdraft penalties on top of the $1,200 in loan

\textsuperscript{50} See supra Part II.2 (displaying a products chart with details about the requirements).
\textsuperscript{51} 12 U.S.C. § 1831(a)(1) (stating that a state bank may not engage as principal in any type of activity that is not permissible for a national bank except in two circumstances, both of which are not relevant here).
\textsuperscript{55} See supra apps. A & B (showing the details of Mr. B’s borrowing).
fees. For example, on the last Thursday and Friday of July 2007, eight checks cleared Mr. B’s account for a total of $2,976 in withdrawals. That more than erased his previous balance of $2,471. So, on Monday, he took out a Direct Deposit Advance of $500.

Alas, that was too little. Even after the loan, Mr. B’s account still had a negative balance of $4.61. When four more checks cleared on Monday, he was socked with $74 in overdraft fees.

Tuesday was worse. A single check for $76 cleared the account, and the bank hit Mr. B with $141 more in overdraft fees. Wednesday brought a bit of relief when three pension checks totaling nearly $3,800 were deposited into the account, erasing a deficit that had climbed to nearly $970. Yet even on that day, the bank assessed another $34 overdraft fee. Additionally, it collected $550 to pay off the principal and finance charge of the $500 Direct Deposit Advance. With a duration of only four days, that loan came at a cost equivalent to a closed-end loan with a 913% APR, counting only the Direct Deposit Advance fees and not the overdraft fees.

Note: Appendix C provides a detailed summary of three months of transactions in Mr. B’s account, including the expensive sequence in late July 2007.

V. THE DIRECT DEPOSIT PUSH: PAST AND PRESENT

In the past 14 years, the federal government has undertaken a major effort to persuade seniors to open bank accounts and use those accounts to receive direct deposits of Social Security and other federal benefits. The government has promoted bank accounts as a safer way for recipients to receive and maintain their benefits. But our estimate that seniors lose at least $700 million of their Social Security benefits annually to fee-based overdraft loans casts serious doubt on this claim. As long as these predatory bank loans exist, seniors will have good reason to avoid bank accounts, as using paper checks has allowed them to maintain control over their funds and keep banks from helping themselves to vital subsistence payments.

Over most of the life of the Social Security program, the government mailed checks to most benefits recipients. This pattern began to change in 1996. In that year, to cut the costs and reduce the paperwork of benefits distribution, Congress passed a law commonly known as “EFT-99” (Electronic Funds Transfer) requiring that most federal payments except tax refunds be made electronically by January 1999.

The government’s efforts to promote direct deposit promised recipients better security and timely payments. For example, in 2005, the Social Security Administration launched a $24-million “Go Direct” marketing campaign to promote direct deposit. The Treasury Department recently estimated that “more than 4.3 million direct deposit enrollments have been achieved since 2005 as a result of the campaign’s activities.” In June 2010, Treasury estimated that 87% of Social Security benefits

and 65% of Supplemental Security Income benefits were issued electronically.\textsuperscript{60} As an alternative for recipients who cannot or will not use bank accounts,\textsuperscript{61} Treasury has established the Direct Express card, a low-cost debit MasterCard developed exclusively for federal benefits recipients. The Direct Express card is a good program which provides a simple, inexpensive and, most importantly, safe mechanism by which unbanked recipients of federal benefits can receive their benefits through direct deposit. Users of the Direct Express card can access their funds at little or no cost, there is no possibility for expensive overdraft or other loan products to be added to the card, and garnishment of funds on the card is prohibited.\textsuperscript{62}

The Direct Express card does have its drawbacks: other funds cannot be added to the card, checks cannot be easily written from the funds on the card, and there is only one free withdrawal. However, by April 4, 2010, over 1 million eligible recipients of benefits from the Social Security Administration had signed up for the program.\textsuperscript{63}

Many recipients still opt to receive their benefits by paper check. In 2003, the government printed and mailed out 170 million checks at an estimated annual cost of $100 million.\textsuperscript{64} In April 2010, the Treasury Department estimated that it mailed out 9.5 million Social Security and SSI checks.\textsuperscript{65} Despite the decline in volume, the annual cost of mailing paper checks was still estimated at $100 million.\textsuperscript{66} In 2009, recipients of Social Security and SSI accounted for more than 92% of the paper benefits checks issued by Treasury.\textsuperscript{67}

A Treasury survey found that some check recipients did not want bank accounts because they were “afraid of incurring high fees as a result of having a bank account.”\textsuperscript{68} At least


\textsuperscript{68}A 2003 survey of Social Security and Supplemental Social Security Income recipients who chose to keep receiving paper checks found that many expressed concerns that “having money deposited directly in the bank seemed to them to take away their sense of control.” Fed. Reserve Bank of St. Louis, Understanding the Dependence on Paper Checks: A Study of Federal Benefit Check Recipients and the Barriers to Boosting Direct Deposit 1, 4 (2004), available
some of those concerns were well founded. Funds direct deposited into bank accounts may be subject to fees for using automated teller machines, overdrafts or account balances that fall below minimum requirements. And direct deposits are not always secure. As a 2008 GAO report warned, “[e]lectronic payments are susceptible to unauthorized use, loss, or theft, just as paper payments, albeit to a lesser extent.” Even in 1996, when it adopted EFT-99, Congress recognized that “many payees rely on these payments for their basic subsistence,” and directed the Treasury Department to undertake its direct deposit effort with extreme care.

In the spring of 2010, Treasury launched a stronger push for electronic distribution of benefits. As of March 1, 2011, new beneficiaries will only be able to receive their funds by direct deposit. Recipients whose benefits started or were filed before that date will be able to continue getting paper checks, but only until March 1, 2013—less than three years from now. At that time, all Social Security payments will be made electronically, with only very limited exceptions. Recipients who do not arrange for the direct deposit of federal funds directly into a bank account will be provided the Direct Express card.

The details of this complete conversion to direct deposit are being worked out in two proposed rules from the Treasury Department. A proposed rule—published on June 17, 2010, with comments due by August 16, 2010—will make it next-to-impossible for beneficiaries to opt out of direct deposit. Currently, a recipient can get a waiver of the direct deposit requirement “[w]here an individual determines, in his or her sole discretion, that payment by electronic funds transfer would impose a hardship due to a physical or mental disability or a geographic, language, or literacy barrier, or would impose a financial hardship.” This flexible standard affords a great deal of individual control; for instance, it allows a beneficiary to receive a paper check and cash it through a relative’s account at no cost to herself or himself and with no risk of the funds being taken by banks for high-cost, short-term loans.


76 31 C.F.R. § 208.4(a).
Additionally, the rule proposed June 17, 2010 would limit waiver of the direct deposit requirement to rare circumstances. Waivers will only be available when recipients meet objective criteria, such as presence in a designated disaster area within 120 days of the disaster. There will be no room for meaningful individual determinations about which arrangement—paper check or electronic deposit—best suits recipients’ needs.

Another proposed rule—published on May 14, 2010, with comments due by July 13, 2010—will permit the deposit of Social Security and other benefits onto prepaid debit cards with minimal consumer protections. So long as the prepaid cards are protected by FDIC insurance and Regulation E (governing electronic funds transfers), under Treasury’s proposal, the cards will be acceptable depositories for federal benefits.

These protections, however, do not adequately address the major concerns surrounding these arrangements. First, at least one bank will make payday loans to holders of prepaid debit cards issued by the bank and co-branded with another financial services company. FDIC insurance protects against the failure of banks, not non-banks in whose name deposits of benefits might be carried at banks. It is unclear what protection, if any, FDIC insurance offers holders of co-branded cards against the loss of their benefits caused by the non-bank. If the co-branding company is a non-bank, and the benefits are carried under this company’s name at a bank, then FDIC insurance would not protect against the bankruptcy of this company. This same concern also arises when a bank makes payday loans to holders of prepaid debit cards from card providers with which the bank has an agreement—as at least one bank does—if these providers are non-banks and carry recipients’ benefits in their names at banks.

Second, users of prepaid cards will be vulnerable to predatory lending, including the bank payday loans that can be obtained through prepaid cards. Recipients can easily be thrown into spiraling debt and lose access to vital subsistence funds, as banks will simply seize funds from the accounts once the benefits are directly deposited into them if the debts are not paid directly.

The continued promotion of the Direct Express Card does not alleviate concerns about other prepaid cards because benefits recipients may choose any prepaid debit card, not just Direct Express, to receive direct deposits. The government push for direct deposit will create huge marketing opportunities for banks to pull recipients into their expensive, high-cost web of credit products—from overdraft products on bank accounts to the bank payday loans offered on both bank accounts and prepaid debit cards.

VI. RECOMMENDATIONS FOR KEEPING FEDERAL BENEFITS SAFE

As the federal government propels seniors and other benefit recipients into mandatory

77 31 C.F.R. § 208.4(c).
80 Management of Federal Agency Disbursements, 75 Fed. Reg. 34394 (proposed June 17, 2010) (to be codified at 31 C.F.R. pt. 208). We understand the Federal Reserve Board is contemplating an expansion of Regulation E coverage to include prepaid debit cards such as those discussed in this report.
use of direct deposit, it has an obligation to make sure the direct deposit vehicles—bank accounts and prepaid debit cards—are safe from high-cost loans.

First, bank regulators, in conjunction with the Consumer Financial Protection Bureau that would be established through the pending financial reform legislation, should adopt and enforce meaningful tests to ensure that banks will offer only responsible small-dollar loan products to their customers. The core criteria for such loans should be the following:\(^81\)

- No lending without an evaluation of the recipient’s ability to afford the payments on the loan;
- An APR, including fees, of 36% or less;
- A term of at least 90 days, or one month per $100 borrowed, depending on the affordability analysis;
- Multiple installment payments rather than a lump sum repayment;
- A prohibition against securing the loans through electronic access to a bank account—which means that recipients cannot be required to agree to electronic repayment, and for those who have agreed, they should be permitted at any time to stop the bank’s access \textit{without cost} from seizing funds from their account.

These criteria will ensure that beneficiaries are able to use bank accounts and prepaid debit cards safely. They will also ensure that precious federal dollars intended to prevent destitution are not transferred directly to financial institutions through exorbitant credit fees and interest.

Second, the Treasury Department should allow direct deposit of Social Security and other benefits only into bank accounts and onto prepaid debit card accounts that do not offer payday loan products. If a bank or prepaid debit card provider offers loans that do not satisfy the five criteria set forth above, direct deposit should not be allowed. Additionally, to make sure that these federal benefits serve their intended purpose of providing for recipients’ necessities, Treasury should forbid banks from helping themselves electronically to Social Security and other exempt benefits as repayment for any loan product.

**CONCLUSION**

As more and more seniors find themselves on the direct deposit bandwagon, the federal government must ensure that they are protected from the predatory loan products being offered as a feature of the accounts into which their benefits are being deposited. Social Security payments are not designed to aid banks scrambling to preserve profit margins and offset lost revenue from fee-based overdraft programs. Social Security is intended to provide seniors with income to cover necessities. For many, Social Security income is critical to pay for basic necessities. The government’s effort to save money by promoting direct deposit must not expose seniors to the indignities and dangers of poverty.

---

\(^81\) See Nat’l Consumer Law Ctr., Stopping the Payday Loan Trap: Alternatives That Work, Ones That Don’t 8-18 (2010), available at http://www.nclc.org/images/pdf/high_cost_small_loans/payday_loans/report-stopping-payday-trap.pdf (detailing the APR, term, installment payment, and no electronic repayment criteria and how adherence to these criteria necessitate that lenders conduct a thorough evaluation of a borrower’s ability to repay).
APPENDIX A

Disclosed APRs Hid Costliness of Wells Fargo Direct Deposit Advances

While Mr. B’s monthly statements told him that he would pay interest at an Annual Percentage Rate of 120 percent to use Wells Fargo’s bank payday loan product, the actual APR for the loans—some of which lasted only two days—was much higher.

<table>
<thead>
<tr>
<th>STATEMENT DATE(s)</th>
<th>DIRECT DEPOSIT TRANSACTION DATE</th>
<th>DIRECT DEPOSIT ADVANCE DATE(s)</th>
<th>DURATION OF DIRECT DEPOSIT ADVANCE (DAYS)</th>
<th>DIRECT DEPOSIT AMOUNT</th>
<th>DIRECT DEPOSIT FINANCE CHARGE</th>
<th>STATED APR (PREMUNING OPEN-END CREDIT)</th>
<th>COMPUTED APR (COMPARABLE TO CLOSED-END LOAN OF SAME DURATION)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/7/07</td>
<td>2/25/07</td>
<td>3/1/07</td>
<td>4</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>913%</td>
</tr>
<tr>
<td>5/7/07</td>
<td>4/20/07</td>
<td>4/27/07</td>
<td>7</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>521%</td>
</tr>
<tr>
<td>8/7/07</td>
<td>7/29/07</td>
<td>8/1/07</td>
<td>3</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>1217%</td>
</tr>
<tr>
<td>9/10/07</td>
<td>8/25/07</td>
<td>8/31/07</td>
<td>6</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>608%</td>
</tr>
<tr>
<td>10/5/07</td>
<td>9/12/07</td>
<td>9/14/07</td>
<td>2</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>1825%</td>
</tr>
<tr>
<td>10/5/07</td>
<td>9/20/07</td>
<td>9/28/07</td>
<td>8</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>456%</td>
</tr>
<tr>
<td>2/7/08</td>
<td>1/21/08</td>
<td>2/1/08</td>
<td>11</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>332%</td>
</tr>
<tr>
<td>5/7/08</td>
<td>4/18/08</td>
<td>5/1/08</td>
<td>13</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>281%</td>
</tr>
<tr>
<td>6/6/08</td>
<td>5/12/08</td>
<td>5/30/08 &amp; 6/2/2008</td>
<td>21</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>182%</td>
</tr>
<tr>
<td>9/8/08</td>
<td>8/20/08</td>
<td>8/29/08</td>
<td>9</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>406%</td>
</tr>
<tr>
<td>11/7/08</td>
<td>10/25/08</td>
<td>10/31/08</td>
<td>6</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>608%</td>
</tr>
<tr>
<td>12/5/08</td>
<td>11/22/08</td>
<td>11/26/08</td>
<td>4</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>913%</td>
</tr>
<tr>
<td>2/6/09</td>
<td>1/22/09</td>
<td>1/30/09</td>
<td>8</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>456%</td>
</tr>
<tr>
<td>3/6/09</td>
<td>2/26/09</td>
<td>3/2/09</td>
<td>4</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>913%</td>
</tr>
<tr>
<td>4/7/09</td>
<td>3/18/09</td>
<td>3/30/09</td>
<td>12</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>304%</td>
</tr>
<tr>
<td>5/7/09</td>
<td>4/25/09</td>
<td>4/30/09</td>
<td>5</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>730%</td>
</tr>
<tr>
<td>7/7/09</td>
<td>6/20/09</td>
<td>6/30/09</td>
<td>10</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>365%</td>
</tr>
<tr>
<td>8/7/09</td>
<td>7/27/09</td>
<td>7/31/09</td>
<td>4</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>913%</td>
</tr>
<tr>
<td>11/6/09</td>
<td>10/25/09</td>
<td>10/30/09</td>
<td>5</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>730%</td>
</tr>
<tr>
<td>12/7/09</td>
<td>11/18/09</td>
<td>11/30/09</td>
<td>12</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>304%</td>
</tr>
<tr>
<td>1/8/10</td>
<td>12/23/09</td>
<td>12/31/09</td>
<td>8</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>456%</td>
</tr>
<tr>
<td>2/5/2010 &amp; 3/5/2010</td>
<td>1/29/10</td>
<td>2/12/10</td>
<td>14</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>261%</td>
</tr>
<tr>
<td>3/5/10</td>
<td>2/16/10</td>
<td>2/26/10</td>
<td>10</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>365%</td>
</tr>
<tr>
<td>4/7/10</td>
<td>3/20/10</td>
<td>3/30/10</td>
<td>10</td>
<td>$500.00</td>
<td>$50.00</td>
<td>120%</td>
<td>365%</td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
<td></td>
<td>196</td>
<td>$12,000.00</td>
<td>$1,200.00</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B

Fees, and More Fees

Even after paying $200 in finance charges for four bank payday loans taken out in a three-month period, Mr. B, a Wells Fargo customer, still got hit with $458 in overdraft penalties.

<table>
<thead>
<tr>
<th>REPORTED ON STATEMENT DATED</th>
<th>TRANSACTION DATE</th>
<th>DATE DIRECT DEPOSIT ADVANCE REPaid OR OVERDRAFT PENALTY ASSESSED</th>
<th>TRANSACTION TYPE</th>
<th>OVERDRAFT PENALTY</th>
<th>DIRECT DEPOSIT ADVANCE AMOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/7/07</td>
<td>7/30/07</td>
<td>8/1/07</td>
<td>Direct Deposit Advance</td>
<td></td>
<td>$500.00</td>
</tr>
<tr>
<td>8/7/07</td>
<td>7/30/07</td>
<td>7/30/07</td>
<td>Overdraft penalty or penalties</td>
<td>$74.00</td>
<td></td>
</tr>
<tr>
<td>8/7/07</td>
<td>7/31/07</td>
<td>7/31/07</td>
<td>Overdraft penalty or penalties</td>
<td>$141.00</td>
<td></td>
</tr>
<tr>
<td>8/7/07</td>
<td>8/1/07</td>
<td>8/1/07</td>
<td>Overdraft penalty or penalties</td>
<td>$34.00</td>
<td></td>
</tr>
<tr>
<td>9/10/07</td>
<td>8/22/07</td>
<td>8/22/07</td>
<td>Overdraft penalty or penalties</td>
<td>$68.00</td>
<td></td>
</tr>
<tr>
<td>9/10/07</td>
<td>8/24/07</td>
<td>8/24/07</td>
<td>Overdraft penalty or penalties</td>
<td>$39.00</td>
<td></td>
</tr>
<tr>
<td>9/10/07</td>
<td>8/25/07</td>
<td>8/31/07</td>
<td>Direct Deposit Advance</td>
<td>$500.00</td>
<td></td>
</tr>
<tr>
<td>10/5/07</td>
<td>9/12/07</td>
<td>9/12/07</td>
<td>Overdraft penalty or penalties</td>
<td>$68.00</td>
<td></td>
</tr>
<tr>
<td>10/5/07</td>
<td>9/12/07</td>
<td>9/14/07</td>
<td>Direct Deposit Advance</td>
<td>$500.00</td>
<td></td>
</tr>
<tr>
<td>10/5/07</td>
<td>9/20/07</td>
<td>9/28/07</td>
<td>Direct Deposit Advance</td>
<td>$500.00</td>
<td></td>
</tr>
<tr>
<td>10/5/07</td>
<td>9/26/07</td>
<td>9/26/07</td>
<td>Overdraft penalty or penalties</td>
<td>$34.00</td>
<td></td>
</tr>
</tbody>
</table>

**TOTALS** |                               |                                                   | $458.00        | $2,000.00      |
Fees, and More Fees (continued)

<table>
<thead>
<tr>
<th>REPORTED ON STATEMENT DATED</th>
<th>FINANCE CHARGE</th>
<th>DURATION OF CREDIT (DAYS)</th>
<th>COMPUTED APR (COMPARABLE TO CLOSED-END LOAN OF SAME DURATION)</th>
<th>APR STATED BY BANK</th>
<th>PRE-transaction ACCOUNT BALANCE</th>
<th>POST-transaction ACCOUNT BALANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/7/07</td>
<td>$50.00</td>
<td>2</td>
<td>1217%</td>
<td>120%</td>
<td>$(504.61)</td>
<td>$(4.61)</td>
</tr>
<tr>
<td>8/7/07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(678.61)</td>
<td>$(752.61)</td>
</tr>
<tr>
<td>8/7/07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(828.61)</td>
<td>$(969.61)</td>
</tr>
<tr>
<td>8/7/07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$2,276.58</td>
<td>$2,242.58</td>
</tr>
<tr>
<td>9/10/07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(103.44)</td>
<td>$(171.44)</td>
</tr>
<tr>
<td>9/10/07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(274.43)</td>
<td>$(313.43)</td>
</tr>
<tr>
<td>9/10/07</td>
<td>$50.00</td>
<td>6</td>
<td>608%</td>
<td>120%</td>
<td>$(313.43)</td>
<td>$186.57</td>
</tr>
<tr>
<td>10/5/07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$218.53</td>
<td>$150.53</td>
</tr>
<tr>
<td>10/5/07</td>
<td>$50.00</td>
<td>2</td>
<td>1825%</td>
<td>120%</td>
<td>$709.72</td>
<td>$1,209.72</td>
</tr>
<tr>
<td>10/5/07</td>
<td>$50.00</td>
<td>8</td>
<td>456%</td>
<td>120%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/5/07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$(50.28)</td>
<td>$(84.28)</td>
</tr>
</tbody>
</table>

$200.00
## APPENDIX C

### An Account on the Edge

Monthly statements from Mr. B’s bank show the expensive fees incurred as he juggled bank payday loans and overdraft coverage in a futile effort to prevent his account balance from falling below zero.

<table>
<thead>
<tr>
<th>Post Date</th>
<th>Balance</th>
<th>Withdrawal</th>
<th>Deposit</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>9-Jul</td>
<td>$3,997.28</td>
<td></td>
<td></td>
<td>Start balance</td>
</tr>
<tr>
<td>11-Jul</td>
<td>$3,497.28</td>
<td>$500.00</td>
<td></td>
<td>ATM—payment to credit card</td>
</tr>
<tr>
<td>11-Jul</td>
<td>$3,397.28</td>
<td>$100.00</td>
<td></td>
<td>ATM—withdrawal</td>
</tr>
<tr>
<td>12-Jul</td>
<td>$3,197.28</td>
<td>$200.00</td>
<td></td>
<td>ATM—withdrawal</td>
</tr>
<tr>
<td>13-Jul</td>
<td>$697.28</td>
<td>$2,500.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>16-Jul</td>
<td>$597.28</td>
<td>$100.00</td>
<td></td>
<td>ATM—withdrawal</td>
</tr>
<tr>
<td>16-Jul</td>
<td>$497.28</td>
<td>$100.00</td>
<td></td>
<td>ATM—withdrawal</td>
</tr>
<tr>
<td>16-Jul</td>
<td>$397.28</td>
<td>$100.00</td>
<td></td>
<td>ATM—transfer to checking</td>
</tr>
<tr>
<td>18-Jul</td>
<td>$297.28</td>
<td>$100.00</td>
<td></td>
<td>ATM—withdrawal</td>
</tr>
<tr>
<td>18-Jul</td>
<td>$247.28</td>
<td>$50.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>19-Jul</td>
<td>$147.28</td>
<td>$100.00</td>
<td></td>
<td>ATM—withdrawal</td>
</tr>
<tr>
<td>20-Jul</td>
<td>$1,556.48</td>
<td>$1,409.20</td>
<td></td>
<td>Mr. B’s paycheck</td>
</tr>
<tr>
<td>23-Jul</td>
<td>$4,556.48</td>
<td>$3,000.00</td>
<td></td>
<td>ATM check deposit</td>
</tr>
<tr>
<td>23-Jul</td>
<td>$3,856.48</td>
<td>$700.00</td>
<td></td>
<td>ATM—payment to credit card</td>
</tr>
<tr>
<td>23-Jul</td>
<td>$3,656.48</td>
<td>$200.00</td>
<td></td>
<td>ATM—withdrawal</td>
</tr>
<tr>
<td>23-Jul</td>
<td>$3,456.48</td>
<td>$200.00</td>
<td></td>
<td>ATM—transfer to checking</td>
</tr>
<tr>
<td>23-Jul</td>
<td>$3,256.48</td>
<td>$200.00</td>
<td></td>
<td>ATM—payment to credit card</td>
</tr>
<tr>
<td>23-Jul</td>
<td>$3,156.48</td>
<td>$100.00</td>
<td></td>
<td>ATM—withdrawal</td>
</tr>
<tr>
<td>24-Jul</td>
<td>$2,786.48</td>
<td>$370.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>24-Jul</td>
<td>$2,571.39</td>
<td>$215.09</td>
<td></td>
<td>Branch store withdrawal</td>
</tr>
<tr>
<td>24-Jul</td>
<td>$2,471.39</td>
<td>$100.00</td>
<td></td>
<td>ATM—withdrawal</td>
</tr>
<tr>
<td>26-Jul</td>
<td>$1,671.39</td>
<td>$800.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>26-Jul</td>
<td>$1,141.39</td>
<td>$530.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>26-Jul</td>
<td>$898.39</td>
<td>$243.00</td>
<td></td>
<td>Check—Verizon Wireless</td>
</tr>
<tr>
<td>26-Jul</td>
<td>$698.39</td>
<td>$200.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>26-Jul</td>
<td>$595.39</td>
<td>$103.00</td>
<td></td>
<td>Check—Verizon Wireless</td>
</tr>
<tr>
<td>27-Jul</td>
<td>$(104.61)</td>
<td>$700.00</td>
<td></td>
<td>Check—Sallie Mae</td>
</tr>
<tr>
<td>27-Jul</td>
<td>$(404.61)</td>
<td>$300.00</td>
<td></td>
<td>Check—Sallie Mae</td>
</tr>
<tr>
<td>27-Jul</td>
<td>$(504.61)</td>
<td>$100.00</td>
<td></td>
<td>Check—Sallie Mae</td>
</tr>
<tr>
<td>30-Jul</td>
<td>$(4.61)</td>
<td>$500.00</td>
<td></td>
<td>Direct Deposit Advance</td>
</tr>
<tr>
<td>30-Jul</td>
<td>$(504.61)</td>
<td>$500.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>30-Jul</td>
<td>$(612.61)</td>
<td>$108.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>30-Jul</td>
<td>$(647.61)</td>
<td>$35.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>30-Jul</td>
<td>$(678.61)</td>
<td>$31.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>30-Jul</td>
<td>$(701.61)</td>
<td>$23.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
<tr>
<td>30-Jul</td>
<td>$(724.61)</td>
<td>$23.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
<tr>
<td>30-Jul</td>
<td>$(747.61)</td>
<td>$23.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
<tr>
<td>30-Jul</td>
<td>$(752.61)</td>
<td>$5.00</td>
<td></td>
<td>Level 2 charge—continuous overdraft</td>
</tr>
<tr>
<td>31-Jul</td>
<td>$(828.61)</td>
<td>$76.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>31-Jul</td>
<td>$(862.61)</td>
<td>$34.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
<tr>
<td>31-Jul</td>
<td>$(896.61)</td>
<td>$34.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
<tr>
<td>31-Jul</td>
<td>$(930.61)</td>
<td>$34.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
<tr>
<td>31-Jul</td>
<td>$(964.61)</td>
<td>$34.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
</tbody>
</table>
## An Account on the Edge (continued)

<table>
<thead>
<tr>
<th>Post Date</th>
<th>Balance</th>
<th>Withdrawal</th>
<th>Deposit</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>31-Jul</td>
<td>$(969.61)</td>
<td>$5.00</td>
<td></td>
<td>Level 2 charge—continuous overdraft</td>
</tr>
<tr>
<td>1-Aug</td>
<td>$811.33</td>
<td>$1,780.94</td>
<td></td>
<td>Mr. B’s military pension</td>
</tr>
<tr>
<td>1-Aug</td>
<td>$2,540.77</td>
<td>$1,729.44</td>
<td></td>
<td>Mr. B’s federal employee pension</td>
</tr>
<tr>
<td>1-Aug</td>
<td>$2,826.58</td>
<td>$285.81</td>
<td></td>
<td>Mr. B’s private employer pension</td>
</tr>
<tr>
<td>1-Aug</td>
<td>$2,326.58</td>
<td>$500.00</td>
<td></td>
<td>Repayment of Direct Deposit Advance</td>
</tr>
<tr>
<td>1-Aug</td>
<td>$2,276.58</td>
<td>$50.00</td>
<td></td>
<td>Finance charge for Direct Deposit Advance</td>
</tr>
<tr>
<td>1-Aug</td>
<td>$2,242.58</td>
<td>$34.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
<tr>
<td>2-Aug</td>
<td>$2,142.58</td>
<td>$100.00</td>
<td></td>
<td>ATM—withdrawal</td>
</tr>
<tr>
<td>2-Aug</td>
<td>$2,042.58</td>
<td>$100.00</td>
<td></td>
<td>ATM—transfer to checking</td>
</tr>
<tr>
<td>2-Aug</td>
<td>$1,942.58</td>
<td>$100.00</td>
<td></td>
<td>ATM—payment to credit card</td>
</tr>
<tr>
<td>2-Aug</td>
<td>$1,842.58</td>
<td>$100.00</td>
<td></td>
<td>ATM—payment to credit card</td>
</tr>
<tr>
<td>3-Aug</td>
<td>$3,251.78</td>
<td>$1,409.20</td>
<td></td>
<td>Mr. B’s paycheck</td>
</tr>
<tr>
<td>3-Aug</td>
<td>$3,074.78</td>
<td>$177.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>3-Aug</td>
<td>$2,974.78</td>
<td>$100.00</td>
<td></td>
<td>Check—credit card payment</td>
</tr>
<tr>
<td>3-Aug</td>
<td>$2,874.78</td>
<td>$100.00</td>
<td></td>
<td>Check—credit card payment</td>
</tr>
<tr>
<td>3-Aug</td>
<td>$2,774.78</td>
<td>$100.00</td>
<td></td>
<td>ATM—withdrawal</td>
</tr>
<tr>
<td>3-Aug</td>
<td>$2,688.78</td>
<td>$86.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>3-Aug</td>
<td>$2,658.78</td>
<td>$30.00</td>
<td></td>
<td>Check—credit card payment</td>
</tr>
<tr>
<td>3-Aug</td>
<td>$2,628.78</td>
<td>$30.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>3-Aug</td>
<td>$2,600.63</td>
<td>$28.15</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>6-Aug</td>
<td>$2,400.63</td>
<td>$200.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>6-Aug</td>
<td>$2,200.63</td>
<td>$200.00</td>
<td></td>
<td>ATM—withdrawal</td>
</tr>
<tr>
<td>6-Aug</td>
<td>$2,071.63</td>
<td>$129.00</td>
<td></td>
<td>Check—AAA</td>
</tr>
<tr>
<td>6-Aug</td>
<td>$1,981.63</td>
<td>$90.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>6-Aug</td>
<td>$1,897.63</td>
<td>$84.00</td>
<td></td>
<td>Check—AAA</td>
</tr>
<tr>
<td>6-Aug</td>
<td>$1,813.63</td>
<td>$84.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>6-Aug</td>
<td>$1,778.03</td>
<td>$35.60</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>7-Aug</td>
<td>$1,742.83</td>
<td>$35.20</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>7-Aug</td>
<td>$1,532.83</td>
<td>$210.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>7-Aug</td>
<td>$1,432.83</td>
<td>$100.00</td>
<td></td>
<td>Check—Retail Services 3</td>
</tr>
<tr>
<td>7-Aug</td>
<td>$1,402.83</td>
<td>$30.00</td>
<td></td>
<td>Check—Retail Services 3</td>
</tr>
<tr>
<td>7-Aug</td>
<td>$1,377.83</td>
<td>$25.00</td>
<td></td>
<td>Check—Retail Services 3</td>
</tr>
<tr>
<td>8-Aug</td>
<td>$1,177.83</td>
<td>$200.00</td>
<td></td>
<td>ATM payment to credit card</td>
</tr>
<tr>
<td>8-Aug</td>
<td>$1,008.05</td>
<td>$169.78</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>8-Aug</td>
<td>$908.05</td>
<td>$100.00</td>
<td></td>
<td>ATM transfer to checking</td>
</tr>
<tr>
<td>9-Aug</td>
<td>$808.05</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>10-Aug</td>
<td>$773.05</td>
<td>$35.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>13-Aug</td>
<td>$573.05</td>
<td>$200.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>13-Aug</td>
<td>$473.05</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>13-Aug</td>
<td>$373.05</td>
<td>$100.00</td>
<td></td>
<td>ATM transfer to checking</td>
</tr>
<tr>
<td>13-Aug</td>
<td>$273.05</td>
<td>$100.00</td>
<td></td>
<td>ATM payment to credit card</td>
</tr>
<tr>
<td>16-Aug</td>
<td>$173.05</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>16-Aug</td>
<td>$73.05</td>
<td>$100.00</td>
<td></td>
<td>ATM payment to credit card</td>
</tr>
<tr>
<td>17-Aug</td>
<td>$1,482.26</td>
<td>$1,409.21</td>
<td></td>
<td>Mr. B’s paycheck</td>
</tr>
</tbody>
</table>
### An Account on the Edge (continued)

<table>
<thead>
<tr>
<th>Post Date</th>
<th>Balance</th>
<th>Withdrawal</th>
<th>Deposit</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>17-Aug</td>
<td>$1,382.26</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>17-Aug</td>
<td>$1,282.26</td>
<td>$100.00</td>
<td></td>
<td>ATM transfer to checking</td>
</tr>
<tr>
<td>17-Aug</td>
<td>$1,182.26</td>
<td>$100.00</td>
<td></td>
<td>ATM payment to credit card</td>
</tr>
<tr>
<td>17-Aug</td>
<td>$1,082.26</td>
<td>$100.00</td>
<td></td>
<td>ATM payment to credit card</td>
</tr>
<tr>
<td>20-Aug</td>
<td>$882.26</td>
<td>$200.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>20-Aug</td>
<td>$837.26</td>
<td>$45.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>20-Aug</td>
<td>$797.26</td>
<td>$40.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>20-Aug</td>
<td>$758.26</td>
<td>$39.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>21-Aug</td>
<td>$893.26</td>
<td>$135.00</td>
<td></td>
<td>Overdraft transfer from credit card</td>
</tr>
<tr>
<td>21-Aug</td>
<td>$475.42</td>
<td>$417.84</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>21-Aug</td>
<td>$175.42</td>
<td>$300.00</td>
<td></td>
<td>ATM transfer to checking</td>
</tr>
<tr>
<td>21-Aug</td>
<td>$75.42</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>21-Aug</td>
<td>$(24.58)</td>
<td>$100.00</td>
<td></td>
<td>ATM payment to credit card</td>
</tr>
<tr>
<td>21-Aug</td>
<td>$(103.44)</td>
<td>$78.86</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>22-Aug</td>
<td>$(137.44)</td>
<td>$34.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
<tr>
<td>22-Aug</td>
<td>$(171.44)</td>
<td>$34.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
<tr>
<td>23-Aug</td>
<td>$(274.43)</td>
<td>$102.99</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>24-Aug</td>
<td>$(308.43)</td>
<td>$34.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
<tr>
<td>24-Aug</td>
<td>$(313.43)</td>
<td>$5.00</td>
<td></td>
<td>Level 2 charge continuous overdraft</td>
</tr>
<tr>
<td>27-Aug</td>
<td>$186.57</td>
<td>$500.00</td>
<td></td>
<td>Direct Deposit Advance</td>
</tr>
<tr>
<td>27-Aug</td>
<td>$86.57</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>28-Aug</td>
<td>$36.57</td>
<td>$50.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>31-Aug</td>
<td>$1,625.10</td>
<td>$1,588.53</td>
<td></td>
<td>Mr. B’s paycheck</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Post Date</th>
<th>Balance</th>
<th>Withdrawal</th>
<th>Deposit</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>31-Aug</td>
<td>$1,910.91</td>
<td>$285.81</td>
<td></td>
<td>Mr. B’s private employer pension</td>
</tr>
<tr>
<td>31-Aug</td>
<td>$1,580.81</td>
<td>$330.10</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>31-Aug</td>
<td>$1,316.62</td>
<td>$264.19</td>
<td></td>
<td>Repayment of Direct Deposit Advance</td>
</tr>
<tr>
<td>31-Aug</td>
<td>$1,080.81</td>
<td>$235.81</td>
<td></td>
<td>Repayment of Direct Deposit Advance</td>
</tr>
<tr>
<td>31-Aug</td>
<td>$880.81</td>
<td>$200.00</td>
<td></td>
<td>ATM payment to credit card</td>
</tr>
<tr>
<td>4-Sep</td>
<td>$2,311.75</td>
<td>$1,780.94</td>
<td></td>
<td>Mr. B’s military pension</td>
</tr>
<tr>
<td>4-Sep</td>
<td>$3,422.49</td>
<td>$1,110.74</td>
<td></td>
<td>Mr. B’s federal employee pension</td>
</tr>
<tr>
<td>4-Sep</td>
<td>$3,322.49</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>4-Sep</td>
<td>$3,222.49</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>4-Sep</td>
<td>$3,122.49</td>
<td>$100.00</td>
<td></td>
<td>ATM transfer to checking</td>
</tr>
<tr>
<td>6-Sep</td>
<td>$3,022.49</td>
<td>$100.00</td>
<td></td>
<td>ATM payment to credit card</td>
</tr>
<tr>
<td>10-Sep</td>
<td>$2,922.49</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>11-Sep</td>
<td>$3,080.49</td>
<td>$158.00</td>
<td></td>
<td>Overdraft transfer from credit card</td>
</tr>
<tr>
<td>11-Sep</td>
<td>$580.49</td>
<td>$2,500.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>11-Sep</td>
<td>$122.49</td>
<td>$458.00</td>
<td></td>
<td>Check</td>
</tr>
</tbody>
</table>
### An Account on the Edge (continued)

<table>
<thead>
<tr>
<th>POST DATE</th>
<th>BALANCE</th>
<th>WITHDRAWAL</th>
<th>DEPOSIT</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-Sep</td>
<td>$(13.97)</td>
<td>$136.46</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>12-Sep</td>
<td>$458.53</td>
<td></td>
<td>$500.00</td>
<td>Direct Deposit Advance</td>
</tr>
<tr>
<td>12-Sep</td>
<td>$358.53</td>
<td>$100.00</td>
<td></td>
<td>ATM transfer to checking</td>
</tr>
<tr>
<td>12-Sep</td>
<td>$258.53</td>
<td>$100.00</td>
<td></td>
<td>ATM payment to credit card</td>
</tr>
<tr>
<td>12-Sep</td>
<td>$218.53</td>
<td>$40.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>12-Sep</td>
<td>$184.53</td>
<td>$34.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
<tr>
<td>12-Sep</td>
<td>$150.53</td>
<td>$34.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
<tr>
<td>14-Sep</td>
<td>$1,559.72</td>
<td>$1,409.19</td>
<td></td>
<td>Mr. B’s paycheck</td>
</tr>
<tr>
<td>14-Sep</td>
<td>$1,059.72</td>
<td>$500.00</td>
<td></td>
<td>Repayment of Direct Deposit Advance</td>
</tr>
<tr>
<td>14-Sep</td>
<td>$959.72</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>14-Sep</td>
<td>$909.72</td>
<td>$50.00</td>
<td></td>
<td>Finance charge for Direct Deposit Advance</td>
</tr>
<tr>
<td>19-Sep</td>
<td>$809.72</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>19-Sep</td>
<td>$709.72</td>
<td>$100.00</td>
<td></td>
<td>ATM transfer to checking</td>
</tr>
<tr>
<td>20-Sep</td>
<td>$1,209.72</td>
<td>$500.00</td>
<td></td>
<td>Direct Deposit Advance</td>
</tr>
<tr>
<td>24-Sep</td>
<td>$209.72</td>
<td>$1,000.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>24-Sep</td>
<td>$109.72</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>24-Sep</td>
<td>$9.72</td>
<td>$100.00</td>
<td></td>
<td>ATM withdrawal</td>
</tr>
<tr>
<td>25-Sep</td>
<td>$(50.28)</td>
<td>$60.00</td>
<td></td>
<td>Check</td>
</tr>
<tr>
<td>26-Sep</td>
<td>$(84.28)</td>
<td>$34.00</td>
<td></td>
<td>Fee—overdraft</td>
</tr>
</tbody>
</table>
Venmo Money, Venmo Problems

The mobile-payment service is trendy, easy to use, and growing fast. But is it safe?

By Alison Griswold

Illustration by Rob Donnelly

Two twentysomethings hop out of a cab. They get dinner. They grab drinks at a bar. Neither stops to worry about splitting the tab. “Just Venmo me,” one says.

Alison Griswold is a Slate staff writer covering business and economics.

That’s how most stories about Venmo, the popular mobile-payment app, begin. First there’s a short anecdote illustrating how Venmo is fast, casual, convenient, and trendy. There might be a moment of conversion: At first, one of those twentysomethings is nervous about sending real money through a mobile app, but after trying Venmo and witnessing its amazing ease and speed, he becomes a proponent of the service as quickly as Venmo became a verb.

This is not one of those stories. It starts, instead, with Chris Grey, a 30-year-old Web developer in New York City, waking up last Thursday to a notification from Chase bank that his account had a pending transaction involving a large sum of money. At first glance, he thought his tax refund must have come through. He’d already paid his rent for the month, so he figured the alert must be for an incoming amount. “Then I did a double take,” he says.

Chase had pinged Grey not about a credit to his account, but a debit for $2,850, through Venmo. Confused, Grey tried to pull up his Venmo account, but his password no longer worked. He used the reset option to get in, then inspected his settings. Under email authentications, a new address appeared. Notifications were disabled. Grey’s payment history showed that the funds—slightly below Venmo’s weekly sending limit of $2,999.99—had been sent at 3:09 p.m. the day before to a user he didn’t recognize. Some text listed the transaction’s ominous-sounding purchase: “for about time.”
Clearly, something was wrong—yet Venmo hadn't notified Grey that anything suspicious could be going on. “I never got an email that my password had changed, that another email was added to my account, that another device was added to my account, or that a lot of my settings had changed,” he says. A colleague and I were able to duplicate this lack of notification with a quick test: Venmo doesn’t alert you if your password or email credentials change from within the account. “There are basic security holes that you could drive a truck through,” Grey says.

These shortcomings should be concerning for any service that handles sensitive financial information, but particularly so for Venmo, which has set its sights on becoming the dominant mobile app for peer-to-peer financial transactions in the United States. In the third quarter of 2014, Venmo processed $700 million in payments—nearly five times the transaction volume it did in the same period a year earlier. Venmo doesn’t share its user numbers, but eBay chief executive John Donahoe has dropped hints. “Venmo is on fire,” he said last month during eBay’s fourth-quarter earnings call. “If you go to any college campus across America, they talk about Venmoing money to each other.”

By making the money transfers quick, uncomplicated, and even cool, Venmo is winning. But for all its promise as a smooth and efficient financial service, Venmo’s popularity seems to be outpacing its customer-support capabilities. As of November, Venmo only had around 70 full-time employees. (Its parent PayPal, which oversaw $64.3 billion in transactions in the last quarter of 2014, has more than 10,000.) Three years after the service left its beta phase, Venmo doesn’t have a dedicated phone line for customer issues. Urgent emails about stolen funds receive slow responses. It doesn’t offer two-factor verification, an increasingly common security layer that requires users to provide a secondary passcode to access an account, though it’s working to implement it. Venmo says its mobile-transfer infrastructure “uses bank-grade security systems and data encryption to protect you and guard against any unauthorized transactions and access to your personal or financial information.” But when a hacker who breaches an account using your password can send $2,850 as quickly and conveniently as a twentysomething can repay $7 for a burrito, that’s clearly not enough.

“These are big problems,” says Rob Shavell, co-founder and CEO of Abine, a data-privacy firm that helps users secure personal information. “There ought to be email warnings, there ought to be two-factor authentication. It’s true for us, it’s true for Venmo, it’s true for all these services.”

Venmo did not respond to multiple requests for comment. Lisa Kornblatt, a spokeswoman for Braintree, the company that acquired Venmo in 2012 and was subsequently bought by PayPal in 2013, on Monday pointed me to PayPal’s security and privacy policies, and didn’t respond to further inquiries. Venmo also declined to speak with me when I stopped by its New York headquarters (which happens to be located one floor above Slate’s office), directing me instead to email press@venmo.com.

Once he realized his account had been hacked, Grey contacted Chase first. To his horror, the bank informed him he’d need to close out the account. Because he’d linked Venmo to his Chase routing number—rather than to a debit or credit card—the account, which he’d had since college, was irreversibly compromised. That meant, in the short term, no access to his money. Grey got to work filing a claim with Chase to dispute the $2,850 withdrawal.

If nothing else, dealing with fraud is something banks are very good at. They have fraud departments to handle problems like Grey’s, and dedicated hotlines for customers to call if something happens. One of the great promises of a credit card is the small customer service number printed on the back. Venmo doesn’t offer that level of assistance. You won’t find a phone number on the contact portion of its website. On the security page, the company advises customers who “suspect that there has been any unauthorized activity” to “contact us immediately at support@venmo.com—we’re here to help.” (You can also tweet @VenmoSupport.) What’s not noted on the security page—but is buried in section C, part 1, small letter n, roman numeral iv of Venmo’s user agreement—is that you should do this immediately,
because if “you contact the Company within two Business Days after learning of the loss or theft, then your liability shall not exceed the lesser of $50.00 USD or the amount of unauthorized transfers that took place on your account before you provided notice to the Company.” After two business days, your liability can jump as high as $500, per Venmo’s terms.

Grey says he went ahead and contacted Venmo almost immediately after learning of the unauthorized activity and reaching out to Chase, at first via the company’s online contact form and then to support@venmo.com. Grey provided Slate with email correspondence showing that he first wrote to the support email address at 11:55 a.m. on Thursday, then again at 6:50 p.m., 7:43 p.m., and finally at 9:38 a.m. on Friday. More than 24 hours after he first contacted Venmo, Grey was still waiting.