<table>
<thead>
<tr>
<th>In This Issue</th>
<th>Lydian Payments Journal</th>
</tr>
</thead>
</table>
| How the Consumer Financial Protection Agency Act of 2009 Would Change the Law and Regulation of Consumer Financial Products  
  By David S. Evans and Joshua D. Wright       | The Lydian Payments Journal publishes articles from thought leaders across the globe on one of the most important industries in the world — payments, the industry which makes trade, the source of all economic prosperity, possible. |
| What You Should Know about the Debit Card in Your Wallet: Where the Federal Reserve’s New Overdraft Rules May Fall Short  
  By Jennifer S. Martin                          | Titled after the Kingdom of Lydia, a region that is now part of eastern Turkey and which is attributed with inventing coinage in 600 BC, the Lydian Payments Journal shapes and chronicles this important sector by focusing on a spectrum of topics: from policy issues such as competition, consumer protection, and interchange to disruptive innovation such as social lending, remittance products, and mobile commerce. |
| Demystifying PCI Technologies                    |                                                                                         |
| By Ulf Mattsson                                   |                                                                                         |
| Banking the Unbanked Using Prepaid Platforms and Mobile Telephones in the U.S.  
  By Francesc Prior Sanz and Javier Santomá      |                                                                                         |
|                                                  |                                                                                         |

This e-journal leverages the power of the Web to provide germane and timely thought leadership to a broad and relevant audience. The online format also works to fuel interaction between readers and authors, extending the dialogue beyond just the articles. Visit the Lydian Payments Journal online at www.pymnts.com/journal.
How the Consumer Financial Protection Agency Act of 2009 Would Change the Law and Regulation of Consumer Financial Products

By David S. Evans† and Joshua D. Wright§

Introduction

As part of its overhaul of financial services regulation the Obama Administration has proposed stronger protection of consumers of financial products and services.1 The Consumer Financial Protection Agency Act of 2009 (CFPA Act), which the Administration submitted to the U.S. Congress on June 30, 2009, would result in a sweeping overhaul of consumer financial protection.2 The CFPA Act would create a Consumer Financial Protection Agency (CFPA) which would assume the responsibility for enforcing most existing consumer financial protection laws from other federal banking regulators as well as the Federal Trade Commission (FTC).3 The CFPA would have significant additional powers to regulate consumer financial products, mandate disclosures, and require covered businesses to offer consumers “plain vanilla” products that the CFPA would design. The legislation would limit federal preemption of nationally chartered financial institutions by allowing states and localities to have stronger restrictions than those adopted by the CFPA and would add a new prohibition against “abusive” practices while allowing new interpretations of existing liability for unfair and deceptive practices. This article details how the CFPA Act would change consumer financial regulation, explores the policy rationale for these changes, and examines how the

† David S. Evans is Lecturer, University of Chicago Law School and Executive Director of the Jevons Institute for Competition Law and Economics and Visiting Professor, University College London.

§ Joshua D. Wright is Assistant Professor, George Mason University and Department of Economics.


3 Id. at § 1011(a).
legislation proposed by the Administration, would affect providers and consumers of financial products and services.4

The Road to 'Stronger' Consumer Financial Product Protection

The CFPA Act consolidates existing consumer financial protection regulation into a new, expansive agency and fundamentally changes longstanding federal laws on consumer financial protection.

A. The Consumer Financial Protection Agency

The United States has passed a number of laws that are in whole or in part designed to provide protection to consumers of financial services products.5 The Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration have responsibility for enforcing these laws for the institutions in their purview in addition to engaging in their main regulatory job of making sure that these institutions meet safety and soundness standards. The FTC also is responsible for preventing unfair and deceptive practices by nonbank lenders such as mortgage companies but not depository institutions and enforcing the Truth-in-Lending Act and others laws against non-depository institutions under Section 5 of the FTC Act. The CFPA Act would transfer the responsibility for enforcing these laws to the new agency and would provide for a process of consolidating the staff of these existing agencies into the new one.

The objective of the CFPA would be to “promote transparency, simplicity, fairness, accountability, and access in the market for consumer financial products or services.”6 The CFPA would obtain additional powers beyond those granted by current laws. The new agency would regulate nearly all consumer financial products and services, regardless of what kind of business provides those products, and would have wide latitude for defining what constitutes a consumer financial product.7 For these products, the CFPA could:

---

4 A number of changes to the Administration’s bill have been proposed as the bill has moved through Congress. The bill that was passed by the House Finance Committee, for example, does not allow the CFPA to punish parties covered by the law from engaging in “abusive practices.” No bill has been adopted by the Senate at this time. Because the legislation is a moving target we focus on the CFPA Act originally proposed by the Administration in this article.

5 The Act enumerates several of these laws, including, amongst others, the Equal Credit Opportunity Act, the Fair Credit Billing Act, and the Gramm-Leach-Bliley Act. Id. at § 1002(16).

6 Id. at § 1021(a).

• prohibit unfair, deceptive, or abusive acts or practices including adopting rules that would prevent such acts or practices;

• prescribe rules for ensuring the disclosure of the costs, benefits, and risks for consumer financial products or services; and,

• define “standard consumer financial products” (also known as “plain vanilla” products), require covered businesses to offer this standard product “at or before the time an alternative consumer financial product or service is offered to a consumer,” and require that consumers to opt out of this standard product before being offered alternative products.

The CFPA would also have various powers to help it achieve its objective of “ensuring that traditionally underserved consumers and communities have access to financial services.” The agency would have the ability to impose civil penalties for violations as well as pursue legal and equitable remedies.

**B. The Unfair, Deceptive and Abusive Conduct Standard**

Federal and state consumer protection law generally prohibit “unfair and deceptive practices.” There is extensive case law interpreting this standard involving both the FTC and state consumer protection legislation. The new agency is not required to define which practices are “unfair” or “deceptive” in a manner that comports with this jurisprudence, nor with the interpretations endorsed by the FTC. The CFPA Act also adds a new standard of “abusive practices” to existing consumer protection regulations for financial products and services. The CFPA Act itself does not define the term “abuse” or “abusive,” but grants the new agency wide latitude to create its own definition.

**C. The Limitations on Federal Preemption**

---

8 Act at § 1036(b)(1).
9 Id. at §§ 1037, 1055.
12 Act, supra note 2, at § 1031.
Much of current banking and lending law preempts states from imposing consumer financial protection laws on federally chartered banks. These federally chartered commercial banks account for 88 percent of commercial bank assets.13 The Act specifically permits states and municipalities to adopt and enforce consumer protection laws against nationally chartered financial institutions so long as these state or local laws provide consumers with protection which is “greater than the protection provided under”14 federal law as determined by the agency.

The Rationale for the Consumer Financial Protection Act of 2009

The CFPA Act would result in a sweeping overhaul of state and federal regulation of consumer financial products and services. Six federal agencies would lose their existing authority, consumer protection would be severed from prudential regulation at five federal banking regulators, and potentially hundreds of consumer protection staff would be transferred to a new agency. This section explains the rationales that have been offered for these changes.

A. Failed Consumer Protection and the Financial Crisis

The CFPA Act is part of the Obama Administration’s proposed reforms of financial services regulation. Those reforms and their rationale are presented in the U.S. Department of the Treasury (Treasury Department’s) Financial Regulatory Reform: A New Foundation.15 In announcing the plan, President Obama suggested that the new consumer protection agency was needed in part because consumers had chosen to take out too much credit; the present financial crisis was in part “the result of decisions made by ordinary Americans to open credit cards and take out home loans and take on other financial obligations.”16 The Treasury Department argued that mortgage and other companies sold products that “were overly complicated and unsuited to borrowers’ financial situation . . . with disastrous results for consumers and the financial system.” Regulation failed because there were multiple agencies and these agencies had a conflict between consumer protection and protection of safe and sound banking practices. The Treasury

13 As of September 2, 2009, total assets of all commercial U.S. banks were $11,060 total assets of all domestically chartered banks were $9,736 (both seasonally adjusted). See Federal Reserve Board, Assets and Liabilities of Commercial Banks in the United States Data—last released September 11, 2009, available at http://www.federalreserve.gov/releases/h8/current/default.htm.

14 Act, supra note 2, at § 1041(a)(2).

15 New Foundation, supra note 1, at 51.

Department concluded that a consumer financial protection agency is needed “to instill a genuine culture of consumer protection.”

The Treasury Department’s report does not provide evidence to support the assertion that failed consumer protection regulation played a significant factor in the financial crisis. There is a consensus that the financial crisis resulted in large part from the collapse of the housing bubble which resulted in the heavy losses to financial institutions that held mortgage-backed securities. As housing prices declined, more consumers defaulted on their mortgages, leading to losses in the value of the securities that included these bad debts. Consumer protection could have reduced these losses to the extent that it could have prevented consumers from taking out mortgages that they then defaulted on. Consumer protection could have prevented predatory lending in which consumers were induced to take mortgages that they could not possibly afford. There is no evidence that we are aware of that predatory lending or other practices that would violate the consumer protection laws resulted in a significant portion of the loss in value of the mortgage backed securities.

17 New Foundation, supra note 1, at 56.


19 Oren Bar-Gill and Elizabeth Warren have argued that “the high proportion of people with good credit scores who ended up with high-cost mortgages raises the specter that some portion of these consumers were not fully cognizant of the fact that they could have borrowed for much less.” See Oren Bar-Gill & Elizabeth Warren, Making Credit Safer, 157 U. PA. L. REV. 1, 39 (2008). They claim that many people who got sub-prime mortgages could have received less expensive prime mortgages. These authors do not provide any evidence that a significant number of homeowners that defaulted would not have done so had they paid lower interest rates. It is doubtful that there would have been fewer defaults since even with lower interest rates these home owners would have had negative equity in their homes and therefore would gain from defaulting. In addition, a Federal Reserve Bank of Boston study finds that most subprime mortgage borrowers would not have received prime mortgages. Christopher L. Foote, Kristopher S. Gerardi, Lorenz Goette & Paul Willen, Subprime Facts: What [We Think] We Know about the Subprime Crisis and What We Don’t (Federal Reserve Board of Boston, Public Policy Discussion Paper No. 08-2, May 30, 2008), available at http://ssrn.com/abstract=1153411. Deterioration of the underwriting standards has also been put to blame for the current crisis. Another study at the Federal Reserve Bank of Boston found that loans issued in 2005–2006 were not very different from loans made earlier, which, in turn had performed well, despite carrying a variety of serious risk factors. While the 2005–2006 loans may have carried risk factors, such as increased leverage, underwriting standards alone cannot explain the dramatic rise in foreclosures. See Kristopher S. Gerardi, Andreas Lehnert, Shane Sherland & Paul Willen, Making Sense of the Subprime Crisis (Federal Reserve Board of Boston, Public Policy Discussion Paper No. 09-1, December 22, 2008), available at http://ssrn.com/abstract=1341853; Geetesh Bhardwaj & Rajdeep Sengupta,
The CFPA Act also provides for stronger regulation of virtually all consumer financial services products and services. There is no evidence that non-mortgage related financial services products played any material role in causing the financial crisis. Credit-card backed securities have fallen in value as a result of the deterioration of the economy and the accompanying rise in credit-card defaults. However, neither these securities nor other consumer financial products to be regulated were part of the derivatives products that caused large financial institutions to teeter on the brink of insolvency in mid-2008.

B. Consumer Mistakes and Irrationality

The proposal to create a new consumer financial protection agency preceded the start of the financial crisis whose beginning is often marked with the collapse of Lehman Brothers in September 2008. Professors Oren Bar-Gill and Elizabeth Warren presented the case for the new agency in an article entitled Making Credit Safer that was published in 2008.

These authors argued that credit markets were failing because “sellers of credit products have learned to exploit the lack of information and cognitive limitations of consumers in ways that put consumers’ economic security at risk.” According to them, “For a growing number of families that are steered into overpriced and misleading credit products, however, credit products only benefit the lenders.” A significant part of the problem is that, “Many consumers are uninformed and irrational.”

Professors Bar-Gill and Warren argue that the existing regulatory agencies are not up to the job of dealing with these problems: “Federal banking regulators have the authority but not the motivation. For each federal banking agency, consumer protection is not first (or even second) on its priority list. By contrast, the FTC makes consumer protection a priority, but it enjoys only limited authority. .. To replace this system they proposed the creation of a “single federal regulator” and a regulatory framework with three


20 These consumer financial products are not identified as contributors to the financial crisis in any of the serious analyses of the crisis that we have seen. See generally Foote et al., supra note 19, at 2-3; 32-34; Gerardi et al., supra note 19, at 2-3, 6-7.


22 Bar-Gill & Warren, supra note 19, at 6.

23 Id. at 5.

24 Id. at 21.

25 Id. at 87.
key elements: “(1) ex ante regulation, rather than ex post judicial scrutiny; (2) regulation by an administrative agency with a broad mandate, rather than by piecemeal legislation; and (3) entrusting the authority over consumer credit products to a single, highly motivated federal agency . . .”

Professor Michael Barr, who is now an Assistant Secretary to the Treasury Secretary leading the efforts on the CFPA Act, proposed some of the key aspects of the CFPA Act in an October 2008 paper.26 He advocated requiring lenders provide a plain vanilla mortgage option to borrowers and imposing “heightened disclosure and additional legal exposure” on those lenders if they persuade a borrower to opt out of the plain vanilla product for another product. He also suggested a new legal standard in which lenders could be held accountable after the fact if they did not provide “reasonable” disclosure to consumers.27

The legal scholars have based their analysis on “behavioral law and economics.” This field claims that consumers act irrationally in predictable ways, that businesses exploit these defects in human reasoning, and that it is possible to design regulations that benefit consumers by reducing the social costs associated with irrational consumer decisions. Members of the behavioral law and economics movement tend to believe in some form of paternalism in which the government can help make consumers make the “right” choices. Soft paternalism “nudges” consumers to make the right decision by, for example, having them ‘opt into’ alternatives that these scholars believe are in the consumer’s best interest.28 Hard paternalism, by contrast, explicitly forbids consumers from making certain choices, such as by preventing sellers from offering some products that consumers would buy.29 The CFPA Act reflects both of these approaches. The new agency would possess the “soft paternalism” tools of forcing lenders to offer “plain vanilla” products as well as the “hard paternalism” tools of forbidding covered businesses from offering certain products consumers find desirable.


27 Id. at 6.

28 One of the leading proponents of “soft” paternalism is Professor Cass Sunstein, who President Obama was recently confirmed to be Administrator of the Office of Information and Regulatory Affairs. See generally Richard Thaler & Cass Sunstein, Nudge: Improving Decisions About Health, Wealth, and Happiness (Yale University Press 2008).

29 Proponents of this approach in fact believe that a number of consumer financial products should be prohibited. See Alan M. White, The Case for Banning Subprime Mortgages, 77 U. CIN. L. REV. 617 (2008) (expounding upon banning several “subprime” lending practices because, amongst other grounds, consumers systematically over-value present-day consumption to future detriment); Owen Bar-Gill, Seduction By Plastic, 98 NW. U. L. REV. 1373, 1425-28 (2004) (advocating mandatory unbundling of transacting and financing services offered by credit card companies and application of state usury laws to credit cards); George Loewenstein & Ted O’Donoghue, We Can Do This the Easy Way or the Hard Way: Negative Emotions, Self-Regulation, and the Law, 73 U. CHI. L. REV. 183, 204 (2006) (advocating ban on credit cards).
Given this history, and the role of advisors to the new Administration in it, it would appear that the rationale of the new consumer financial protection agency is based on the view that consumers make systematically bad decisions when it comes to consumer lending products. The CFPA, according to this view, is needed to prevent consumers from making those bad choices and to deter businesses that provide consumer financial products from exploiting the tendency of consumers to choose products that are not in the consumers’ best interests.

The Effect of the Consumer Financial Protection Act of 2009 on the Provision of Consumer Credit

It is impossible to say with certainty how new laws and regulatory authorities will ultimately affect the marketplace. In the case of the CFPA Act much depends on how the courts interpret the Act, who the President appoints to lead the new agency, and what policies this leadership pursues. Several aspects of the CFPA Act, however, make it likely that the CFPA Act would result in consumers paying more to borrow money and having less choice in how to borrow money.\(^3\) This section explains the basis for our concerns.

Lenders can expect to earn profits from providing credit to consumers when the interest rate returns they receive, after adjusting for the possibility of default, exceed the sum of the cost of the capital they are providing to consumers and the other costs and risks associated with making that loan. Lenders offer particular lending products when the overall expected returns from consumers that use that product—say an adjustable rate mortgage that is fixed for three years and variable annual for 27—exceed the cost of capital, servicing costs and other fixed costs of making the product available, by enough to provide an adequate return on investment.

Loans vary greatly in their risks because borrowers vary in their creditworthiness and because some loans lack collateral for the lender to fall back on. Financial institutions expend a great deal of effort to design products, and to make lending decisions, to customize the interest rates and other fees to the creditworthiness of the borrower. Consumer credit is one of the most heterogeneous products in the economy.

The CFPA Act would have various effects on the decisions of providers of consumer financial products to supply consumer credit to particular consumers, the types of products they would offer, and the interest rates and fees they would charge.

\(^3\) We focus on lending, which is just one of the financial products and services covered by the Act of 2009, because of its importance to consumers and the economy overall.
The CFPA Act would result in two radical changes in consumer protection law that affect consumer lending. First, the CFPA Act introduces a new liability for “abusive” lending practices and effectively permits new interpretations of longstanding restrictions on “unfair and deceptive” practices. Specifically, the CFPA Act authorizes the new agency to take any authorized action to “prevent a person from committing or engaging in an unfair, deceptive, or abusive act or practice under Federal law in connection with any transaction with a consumer for a consumer financial product or service.” The CFPA does not have to adhere to the FTC-related jurisprudence on unfair and deceptive practices. In addition the CFPA Act itself does not define the term “abusive,” thereby giving the new agency wide latitude in identifying as abusive any practice that it views as suspect. Without requiring harmonization with FTC interpretations of “unfairness” or “deception,” the CFPA interpretations of these terms, as well as the new authority to prohibit undefined “abusive” practices, would raise issues that would need to be resolved through the courts over time. That would create considerable legal uncertainty for financial institutions that would face unknown and unquantifiable liabilities.

Second, the CFPA Act specifically allows states and municipalities to adopt more stringent regulations than those adopted by the CFPA itself. Rather than providing a uniform set of regulations, the CFPA effectively provides a “floor” on regulation. The Treasury Department’s Financial Regulatory Reform plan seems to suggest that the CFPA would encourage State enforcement actions. Consumer protection requirements for lending products could vary across states and possibly municipalities. That is a likely outcome based on other situations where federal law does not preempt state and local laws, including state antitrust and consumer protection law. Moreover, historically the FTC has imposed important restraints on the judicial interpretation of state consumer protection legislation and thereby encouraged uniformity among states in

31 Act, supra note 2, at § 1031.

32 New Foundation, supra note 1, at 63.

33 At least one Federal Trade Commissioner has expressed concerns about this feature of the CFPA. See William E. Kovacic, Statement on the Proposal to Create a Consumer Financial Protection Agency to the Committee on Energy and Commerce and the Committee on Financial Services (July 28, 2009), available at http://www.ftc.gov/speeches/kovacic/090728sttmrecord.pdf. Commissioner Kovacic notes that “conflicts in interpretation and in litigation strategies, along with an increase in litigation over jurisdictional questions, will adversely affect every core area of consumer protection for which the FTC will continue to exercise primary responsibility.” Id.

34 New Foundation, supra note 1, at 50-51.

35 Id. at § 1041(b).
addition to consistency with the federal government. The CFPA Act would limit those constraints and thereby permit a greater degree of variety and inconsistency.  

We do not believe that it is an exaggeration to say that the combination of these two features would likely lead to an exponential increase in the costs and risks associated with litigation and regulation related to consumer lending products. Financial institutions would have to invest resources to comply with potentially incompatible regulations across many federal, state and local jurisdictions, incur the cost of litigation and regulatory actions in many jurisdictions, face a potentially greater liability depending on the eventual interpretation of unfair, deceptive and abusive practices, and bear the uncertainty of how the CFPA, states, localities and ultimately the courts will define unfair, deceptive, and abusive practices. For financial institutions these changes in consumer protection law would raise the expected cost of consumer lending and therefore lead lenders to raise interest rates and fees. Some financial products would be withdrawn or not offered because they would not be profitable in the face of these costs.

The CFPA Act would also create a new agency that, if it proceeds as its proponents advocate, would impose significant costs on lenders for regulatory reviews and negotiations concerning mandatory disclosures particularly for the introduction of new products. The CFPA’s powers concerning “plain vanilla” products could result in the most consequential effect on the cost and profitability of lending products. The CFPA could design standard products and require providers of consumer financial products to offer those products first to customers and possibly even require consumers to explicitly opt out of the CFPA product before allowing the lender to offer the consumer its own product. This would take a great deal of discretion over the design of lending products and put it in the hands of a regulatory agency with little knowledge of how those design decisions affect the profitability of lending. In some cases one could imagine a financial institution deciding not to offer a new product because of the risk that the CFPA would mandate the offering of a version of its own that would make the new product unprofitable. In other cases, it is possible that lenders would decide not to offer certain products to some consumers because of the prospect that these consumers would take unprofitable plain vanilla versions of those products.

Rather than protecting consumers, the CFPA Act runs the risk that it would instead harm consumers by making it harder and more expensive for them to obtain credit. Consumers would have to pay more to borrow to cover the increased costs of lending described above. It is also likely that consumers would not


37 See Act, supra note 2, at §§ 1036(b)(1)(B); 1036(b)(2).
be able to borrow in some ways available today because the CFPA would prohibit those methods or because financial institutions would find that those products unprofitable as a result of the increased costs and the requirement to offer the CFPA-designed products to consumers.

Consumers have benefited from the increased availability and democratization of credit over the last 30 years. That expansion of credit came about in part because of the relaxation of regulations that prohibited certain credit products. Consumers in the high-inflation years of the late 1970’s were unable to obtain affordable adjustable rate mortgages because they were largely prohibited. Meanwhile state interest rate regulation prevented the emergence of a national market in credit cards and made credit card lending unprofitable for many consumers, particularly ones with poor credit, in many states. Over time consumers have been able to borrow in increasingly more affordable ways as a result of financial innovations. The CFPA Act risks returning the country to an earlier time in which credit was available only to the most qualified individuals for whom financial institutions were most assured they could extend profitable loans.

Conclusion

The CFPA Act would fundamentally change consumer financial protection law and regulation in the United States. It would lead to a remake of consumer protection law through a new “abusive practices” concept and provide for new and expansive interpretations of unfair and deceptive practices; enable and perhaps encourage states and localities to adopt more stringent but not necessarily consistent consumer protection laws; and create a powerful agency that could, among other things, design its own lending products and force lenders to push those products on consumers. Consumer financial protection is important and the

---


40 Christopher C. DeMuth, The Case Against Credit Card Interest Rate Regulation, 3 YALE J. ON REG. 201 (1986); David S. Evans and Richard Schmalensee, Paying with Plastic: The Digital Revolution in Buying and Borrowing (MIT Press, 2005).

41 Evans and Wright, “An Assessment…”, supra note 38, at 40-43.
recent financial crisis has revealed some areas in which protections could be improved. The proponents of the CFPA Act have not, however, provided much in the way of explanation or evidence as to why this sweeping overhaul of consumer financial protection is needed now or why it would benefit the public. The Act, as proposed by the Administration, would most likely result in a significant reduction in the availability of credit to consumers and the reversal of long-term trends towards the democratization of credit in the United States.
What You Should Know about the Debit Card in Your Wallet: Where the Federal Reserve's New Overdraft Rules May Fall Short

By Jennifer S. Martin†

Introduction

Bank debit cards may look like credit cards, but they certainly do not act like them when it comes to account overdrafts. This does not suggest that credit cards are better than debit cards, as complaints abound concerning the transparency of fees charged to consumers for credit card transactions as well. Nevertheless, consumers are more familiar with the workings of credit cards, often not realizing that credit and debit overdraft charges work differently. First, many credit card companies will deny a customer charge at the counter if the charge would result in the customer exceeding her credit line. Second, if the bank approves the credit card charge regardless and permits the consumer to exceed her credit line on a credit card, the typical bank imposes a charge averaging well over $27.00. This credit card over-the-limit fee, however, is a monthly charge, rather than a per-transaction charge that is commonplace for debit card transactions that exceed a customer's bank account limit.

Bank overdraft services operate at high costs to consumers. According to the Consumer Federation of America, the average national overdraft fee at the ten largest banks is $34.65, with $1.75 billion in annual fees paid by consumers to banks for overdrafts resulting from checks, debit card purchases, automated

† Jennifer S. Martin is Visiting Associate Professor of Law, University of Oregon School of Law. Professor Martin can be reached at jsmart@uoregon.edu. J.D. Vanderbilt University School of Law; B.S. University of Nevada, Las Vegas. Portions of this article are based on an article that first appeared in the Memphis Law Review in 2009. See generally Jennifer S. Martin, How Your $4 Cup of Coffee Can Cost You $39 or More If You Use Your Debit Card! Federal Level Consumer Protection and Modern Payments Transactions, 39 Memphis L. Rev. 805 (2009).

1 See Testimony of Adam J. Levitin Associate Professor of Law Georgetown University Law Center before the Committee on Senate Banking, Housing and Urban Affairs (Feb. 12, 2009) (arguing that the lack of transparency costs American consumers $12 billion in unnecessary interest and fees in 2007).

teller machine (ATM) withdrawals, and preauthorized transactions. Very few banks have caps on the amount of overdraft fees that can be charged in a single day on debit transactions, and those that do cap fees have very high daily limits. For example, Bank of America caps its daily overdraft fees at $245. While some large banks also often “batch” reorder daily transactions from highest to lowest, a process that increases the number of overdraft fees banks charge, others such as JP Morgan Chase are trying to get ahead of proposed legislation by abandoning the practice.

Currently, customers often have debit card overdraft protection that they don’t ask for, as banks typically enroll customers in debit card overdraft protection automatically without affirmative customer consent or request. The practice of overdraft protection on debit card transactions persists even though many overdrafts occur on small debit card transactions for which consumers might genuinely prefer the bank deny on the spot, rather than get a $34 overdraft charge. Accounts held by young adults and those with low-income account for the largest portion of overdraft charges, with most overdrafts occurring on point of sale (POS) debit transactions.

The federal government has hardly noticed consumer issues related to newer payment systems such as debit cards until recently. Much of the current world that we know with debit cards is about to change. In early 2009, the Federal Reserve Board, along with the Office of Thrift Supervision (OTS) and the National Credit Union Administration (NCUA) (collectively, the Agencies), proposed new rules under the Electronic Funds Transfer Act (EFTA), implemented pursuant to Regulation E, which the Agencies “intended to ensure that consumers have clear and timely information about their account balances, so that they can properly manage their accounts and avoid unexpected overdraft charges” (Proposed Overdraft Rules). Somewhat oddly, the Agencies proposed not just one, but rather, two proposed alternative rules: (i) an opt-out rule whereby a bank could not charge overdrafts unless the bank first gave the consumer notice of the fees and an opportunity to opt-out; and (ii) an opt-in rule whereby the bank could only charge overdraft fees if the consumer opts-in to the bank’s overdraft services.

---

5 FDIC Study, supra note 2, at v. For accounts held by young persons (ages 18 to 25), 46.4% had NSF activity. Id. For accounts held by low-income customers, 38% had at least one NSF transaction. Id.
In a surprising turn of events, the Federal Reserve’s final rules came down mostly on the side of consumers on most of the overdraft issues (Final Rules). The new rules, which banks must implement by July 1, 2010, prohibits banks from charging an overdraft fee on ATM and POS transactions without the customer affirmatively opting-in to overdraft protection. In a defeat for the banking industry, the new rules apply to existing and new accounts and banks must offer the same terms to consumers who do not opt-in to overdraft services. Moreover, banks must offer the same account terms to customers who do not choose overdraft protection for ATM and POS transactions. The Final Rules did not address all issues raised by consumer groups, such as bank holds on certain POS transactions and batch reordering of transactions.

This essay supports the opt-in regulatory mechanism for overdraft fees of the general type adopted by the Federal Reserve, particularly because the multi-tiered approach adopted recognizes that consumers may desire to have overdraft protection on some items, such as paper checks, but may not desire the same protection for ATM and POS transactions. The Final Rules may fall short of achieving transparency in consumer transactions because the Final Rules: (i) do not require disclosure of the annual percentage rate (APR) on overdrafts which might contribute to confusion; (ii) do not eliminate certain banking practices that operate to increase fees on consumer accounts for those who opt-in to overdraft protection, such as bank holds for purchases like gasoline and restaurants and batch reordering of daily transactions; and (iii) do not allow consumers to choose if they want check and ACH overdraft protection. Moreover, the Final Rules do not address the size or fairness of overdraft fees. The failure of the Federal Reserve to timely and adequately address consumer protection deficiencies, such as those related to debit cards, is not a signal that they are unimportant to regulation of the financial industry. Rather, it may be a signal that a closer look at the regulatory structure for consumer transactions is in order.

The Problem of Debit Card Transactions

Bank customers using modern payment methods like debit cards face the challenge of deciding whether their account has sufficient funds to make a purchase in a system where overdraft fees are high and bank practices are often unclear. While those whose accounts never run low may have little concern about overdraft fees, the methods banks employ for enrolling consumers and imposing fees can be costly for those on the brink of a negative balance. Without complete information, particularly about the practices of each bank, it is difficult to know if any one consumer can use a debit card at a POS transaction or would be...

---

better using cash or another form of payment. Unfortunately, at least until July 1, 2010, consumers with low account balances may be better off not using debit cards at all.

A. Banking Methods of Charging Overdrafts

Deciding whether a consumer should use a debit card or other payment method for a POS transaction depends greatly on the terms of the bank account, what type of overdraft protection the account has for non-sufficient-funds (NSF) transactions, and the bank’s method for charging overdrafts. The banking industry drafts the contract clauses that form the basis for customer account agreements. While freedom of contract (private ordering) dominates consumer depository accounts, some government oversight creates limited consumer protections for those using account services, primarily disclosure-based requirements. Accordingly, an examination of the account programs banks offer to consumers under the terms of their depository accounts is helpful.

Banks commonly offer consumers three types of overdraft programs for their accounts: automated, linked-accounts, and line-of-credit (LOC). Automated overdraft programs use computerized bank procedures to determine if an NSF transaction qualifies for overdraft coverage. If coverage is available, the bank pays the item and charges the consumer a fee. Linked-account programs allow the bank to move money from another account of the consumer, typically a savings account, when the primary account has an NSF transaction. Where there is a linked-account, the bank typically charges a fee for the transfer made to cover the overdraft. A line of credit overdraft program is a contractual agreement between the bank and the customer for the bank to lend a specified amount to cover NSF items, charging a stated rate of interest for the amount advanced.

According to a 2008 Federal Deposit Insurance Corporation (FDIC) study, banks often automatically enroll customers in overdraft protection both for their paper checks and for ATM and POS transactions when they open an account. Customers have to ask for overdraft protection for linked-accounts and must apply and qualify for a LOC program. That is, banking practice for overdrafts utilizes an opt-out system for the more expensive automatic overdraft coverage associated with primary accounts and an opt-in for the less expensive programs of linked-accounts and LOC. These standard practices have historically resulted in higher fees to consumers and placed the onus on the consumer to recognize the difference between the types of overdraft protections.

---

8 See, e.g., Electronic Funds Transfer Act, 12 C.F.R. §205.1 (2009) (“primary objective . . . is the protection of individual consumers engaging in electronic funds transfers”); Regulation DD, 12 C.F.R. 230 (2009) (“primary purpose . . . is to enable consumers to make informed decisions about accounts at depository institutions”).
Among the banking practices most likely to affect consumer accounts are those allowing an overdraft at an ATM or POS debit transactions, but not informing the customer or the seller that the transaction will cause an overdraft of the account. Other banking practices include daily “batching” and vendor debit holds. Daily “batching” is done by a large number of banks by bundling multiple transactions together for processing at some point in the day and then reordering the transactions to increase the number of overdrafts on the account. Vendors such as gasoline stations, hotels, and restaurants place temporary holds on consumer accounts that can linger for days when consumers use their debit card for transactions, even when the actual purchase is smaller, laying the foundation for a potential overdraft if the consumer believes the money is available.

Consumer accounts are dominated by the terms and practices banks offer. While contractual private ordering ordinarily presumes assent to the agreement, consumers may not know which policies and practices affect their account. Because private ordering of banking relationships between consumers and banks does not always result in full knowledge of account terms, consumer protection regulations form an important component when evaluating a consumer’s use of their debit card.

**B. Overdraft Fees Under the Final Rules**

In recent years, banks have expanded the number of types of transactions and customers covered by overdraft services. Consumers need assistance “in understanding how overdraft services provided by their institutions operate and to ensure that consumers have the opportunity to limit the overdraft costs associated with ATM withdrawals and one-time debit card transactions where such services do not meet their needs.” Under the existing structure, banks can readily enroll customers in overdraft protection and impose fees for NSF transactions. The consumer caught unaware has little choice but to pay the fees. The Final Rules are designed to address at least some of the common consumer complaints about overdrafts.

The Final Rules represent a historic change in regulatory approach to ATM and POS overdraft fees, which banks have operated subject to little federal oversight thus far. Most importantly, under the opt-in mandate of the Final Rules, beginning July 1, 2010, banks can no longer readily enroll customers in overdraft protection and then impose NSF fees when a consumer makes a transaction not knowing about the program. Moreover, banks cannot depend on prior “enrollment” of consumers with existing accounts, but will have to secure consumer approval even for these accounts before imposing overdraft fees on ATM

---

9 Electronic Funds Transfer Act, *supra* note 8, at §215.

10 12 C.F.R. § 205.17(b).
and POS transactions. In the event that a consumer does opt-in and changes his mind, the bank must allow the consumer to opt-out at a later date. Finally, banks may not tie the payment of overdrafts on checks to overdrafts on ATM and POS transactions and must offer consumers who do not want overdraft coverage the same account terms and conditions as those who choose the service.

While the Final Rules adopt a consumer-friendly opt-in approach, issues remain. First, with billions of dollars of revenue on the line, banks may attempt to encourage consumers, subtly or overtly, to choose overdraft protection that covers the ATM and POS transactions. This may inadvertently occur if consumers are not able to fully understand the model disclosure forms or receive disclosure on how banking practices affect the provision of the service. For instance, because the Agencies do not propose to treat overdraft fees as loans subject to TILA, consumers may not realize that a $27 overdraft fee charged on a $20 debit transaction repaid in two weeks represents an APR of 3520%. The APR on other overdrafts could be substantially more, especially if the transaction is smaller and the consumer returns the account to a positive balance the very next day. Second, a short, one page form will not explain to consumers how bank practices, such as batch reordering of transactions or account holds, affect the costs associated with the service if the consumer opts-in. Batch reordering and account holds are not covered by the Final Rules. Third, the Final Rules are disclosure, rather than merit based regulations, so they do not address the size of overdraft fees charged by banks, and do not create any specific rights to challenge the size of the fee.

II. Solving the Problems of Consumer Depository Accounts

The largest problems facing regulation of consumer depository accounts are ones created by the need to keep regulations in pace with innovation. That is, bank innovation results in products on the marketplace that are either completely new or are comprised of such variation that the products might as well be new. Services associated with debit cards are a perfect example because debit cards were not commonplace until the late 1990s. Debit cards attach to regular bank depository accounts, yet are not checks, pure ATM cards, or even credit cards. Due to the changing nature of banking products, any “regulatory measures are temporary expedients, not eternal verities . . .”11 With respect to debit cards, innovation has progressed unchecked in the wake of consumer excitement for the innovation itself, without creating a parallel regulatory framework. Accordingly, any discussion of the issues of consumer depository accounts should

take up an examination of the relationship between consumers and banks and explore possible improvements to existing regulatory structure so it may better adapt to innovations in banking products.

Although Regulation E and Regulation DD provide limited consumer protections, the contract with the banking institution primarily controls account features like debit cards. Contract law is versatile, flexible, and adaptable. Despite the flexibility of contracts that has permitted the innovations regarding POS transactions to become commonplace, the contract paradigm has limitations.\(^\text{12}\) While agreement by contract may appropriately govern account aspects, the core of the contract problem with debit cards concerns the basic contract principal of autonomy: whether the consumer \textit{actually} assents to the bank service. There is doubt whether the bank and consumer relationship satisfies ordinary notions of autonomy in debit card transactions, making arguments in favor of the Final Rules that enhance consumer choice more persuasive.

Autonomy is the basis of mutual assent and traditionally anticipates that parties can determine with some level of certainty the extent of their contractual promises. Mutual assent is at the heart of the overdraft fees controversy. Understandably, there is mutual assent when customers voluntarily open depository accounts and request a debit card as part of the account. However, voluntary agreement for related services like overdraft protection is less certain if many banks automatically enroll customers in the overdraft protection service without consumers’ request, a practice the Final Rules addresses. The disproportionate effect that overdraft fees have on those least able to pay them, young adults, seniors, and those in low-income areas, supports the Federal Reserve’s adoption of an opt-in rule regarding bank overdraft fees.

Full disclosure of the benefits and detriments of the programs prior to an \textit{active enrollment} decision is the best approach. If under the Final Rules a consumer enrolls in overdraft protection, resolution of assent and fairness hinges upon the disclosure of the terms of the overdraft service and the practices involved in securing assent. For instance, even though Regulation DD affirmatively requires disclosure of fees, the GAO found that consumers have difficulty obtaining account terms and conditions and complete fee information even when requested.\(^\text{13}\) Moreover, even if the bank discloses the fees, the government does not regulate


the reasonableness of fees or the manner in which they are imposed. The terms of overdraft fees are most likely ones of “adhesion,” in that they are offered or imposed without the ability to negotiate them: “take it or leave it” terms. If the GAO is correct, then banks often fail to disclose the terms at all, even when asked. So, will the Final Rules result in substantial changes in banking practices?

Disclosure is at the cornerstone of most consumer regulations and is the primary prong of financial regulation. The Final Rules address disclosure issues primarily through the model opt-in form (the form) that accompanies the rules. Importantly, the form: (i) requires that banks affirmatively give customers knowledge of enrollment in overdraft services; (ii) specifies the fee amounts that a bank charges per overdraft transaction, any daily fee charged for the account being overdrawn, and any daily limits on overdraft fees; and (iii) contains information about other, less costly banking services and where the consumer can obtain more information. These changes are significant because under current practice banks enroll many consumers without their knowledge or consent and without such disclosures. Upfront disclosure is a key feature of the Final Rules, especially since consumers sometimes have difficulty obtaining fee terms at many banks despite Regulation DD requirements of fee disclosure. Of course, no form is perfect and there remains the potential for consumer confusion.

Curbing bank practices that disadvantage consumers by increasing the amount of overdraft fees incurred is the second prong in the solution to the problems with overdraft protection services banks currently offer. On this point, the Final Rules fall short. Although the Proposed Overdraft Rules addressed the issue of debit card holds by reducing many of the holds from days to just hours, the Final Rules contain no restrictions on holds, leaving wide discretion for the length and size of holds. It is doubtful that a consumer who goes out to gas up the car and buy groceries will know that in order to avoid an overdraft fee caused by a two hour gas pump hold on their card, he or she may want to buy groceries before gas when account balances are low. The Final Rules also do not take up other banking practices that increase the amount of overdraft fees, such as batch reordering of transactions from largest to smallest.

The final prong of any solution regarding overdraft fees must address the size and number of fees imposed for consumers who opt-in the service. While banks typically impose credit card over-the-limit fees on a monthly basis, banks charge overdraft fees on a per-transaction basis. Some consumers may continue to believe that credit and debit cards work the same in this respect. Consumers also tend to believe that government regulation is merit oriented, rather than disclosure based. While some in Congress have urged

http://www.gao.gov/new.items/d08281.pdf (less than 40% of banks provided account terms and conditions when the GAO personnel visited bank branches and less than 25% provided comprehensive fee information).
restrictions on overdraft fees to a “proportional” amount, the Final Rules do not take up fee size. To the extent that some banks charge overdraft fees on NSFs of less than $5, the size of the fee imposed is clearly material to consumers. Some banks have altered current practices to address this issue.

While the Final Rules represent an improvement over the status quo in terms of informing consumers about enrollment in overdraft services, they do not represent a complete solution to open issues of debit and ATM overdrafts. From the industry perspective, there are genuine operational issues at some banks that will require retooling of existing systems. Much of this must take place by July 1, 2010. Despite the successes in the Final Rules, consumers should not believe that they represent a panacea for overdrafts. If they do, disappointment will follow. This type of regulation is long overdue, probably owing to the more recent development of the product and regulatory system’s inability to respond effectively and promptly to developing issues in newer products. At its simplest, a solution to the problems of consumer choice and disclosure in debit card overdrafts favors a default rule system that gives the consumers an arrangement with the lowest cost. Despite the criticisms herein, the Final Rules go a long way toward that goal.

**Conclusion**

“Like all other questions, the question of how to promote a flourishing society . . . [should] be answered as much by experience [as by] theory.”¹⁴ What does experience show when consumer complaints abound regarding overdraft fees charged for ATM and debit transactions? Full disclosure enhances consumer choice, a point on which the Final Rules makes progress. The heavy cost of overdraft services on debit and ATM transactions in comparison to the cost of the items that cause the account to be overdrawn dictate that regulatory leadership is necessary. The Federal Reserve should not, however, avoid the shortcomings of banking practices that increase overdraft fees in ways that consumers would not anticipate and that are harsh.

Though the current economic climate sharpened the need for reforming financial oversight, the ultimate course of conduct that will provide “robust consumer protections” in the long term remains unclear. The proper blend of market and government regulation is still the subject of active debate. As we face an aged regulatory structure that has become less responsive to the current marketplace, embracing a long-term strategy of some type is a necessity. Yet, “Some truths are so basic that, like the air around us, they are easily overlooked.”¹⁵ Market regulation dependent upon the transparency of transactions has little room

---


for practices that undermine the same transparency and consumer choice. Even when the Final Rules come into force, the failure to achieve greater transparency suggests the best practice for most consumers will be not to choose debit and ATM overdraft services. Until then? Use your debit cards with care.
Demystifying PCI Technologies

By Ulf Mattsson†

June 30, 2007 was a big day for data security. That was the deadline for organizations that store, process, or transmit credit card payments to be in compliance with the Payment Card Industry Data Security Standard (PCI DSS). As the deadline approached, the media reported that less than half of all affected businesses would be able to meet that deadline.

People in the security industry shook their heads and wondered why businesses were struggling so hard to comply with what we saw as very basic, common-sense security measures. We couldn't figure out why even the stiff penalties for noncompliance – fines of up to $500,000 and loss of the ability to accept credit cards – apparently wasn't enough to get affected businesses to take security seriously. And then we went right back to writing unintelligible documentation for data security programs. We cranked out mountains of articles and white papers intended to make the technologies necessary for PCI DSS compliance understandable to the general public; unfortunately we wrote them in geek, which is about as understandable to most people as Greek.

Perhaps that's why, a year and a half after the deadline, businesses are still struggling with PCI compliance. A recent Ponemon Institute PCI-DSS Compliance survey revealed that only 28% of smaller companies (501-1000 employees) are PCI-DSS compliant and around 70% of large companies (75,000+ employees) say they are in compliance. Those are horrible statistics.

Compliance can be achieved with little or no angst if you understand what you need to do and the tools that enable you to do it. In this article we will review the PCI standard and take an in-depth look at the more critical data protection technologies.

† Ulf Mattsson is the Chief Technology Officer for Protegrity, a leading provider of Data Security Management Solutions. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development, and a consulting resource to IBM's Research and Development organization. Ulf holds a degree in electrical engineering from Polhem University, a degree in Finance from University of Stockholm, and a master's degree in physics from Chalmers University of Technology.
Reviewing the Payment Card Industry Data Security Standard

The Payment Card Industry (PCI) Data Security Standard was created by major credit card companies to safeguard payment card data. Visa, MasterCard, American Express, and other credit card associations mandate that merchants and service providers meet certain minimum standards of security when storing, processing, and transmitting cardholder data. Merchants, service providers, and banks are required to perform an annual assessment (for Level 1 merchants), and annual penetration testing and application testing (for Level 1 and 2 service providers). All credit card processing systems require logging of all access to credit card data, in addition to quarterly scans and annual penetration tests.

The PCI DSS is a multifaceted security standard centered around six best practice principles and a set of associated requirements:

- **Build and Maintain a Secure Network**
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- **Protect Cardholder Data**
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks

- **Maintain a Vulnerability Management Program**
  - Requirement 5: Use and regularly update anti-virus software
  - Requirement 6: Develop and maintain secure systems and applications

- **Implement Strong Access Control Measures**
  - Requirement 7: Restrict access to cardholder data by business need-to-know
  - Requirement 8: Assign a unique ID to each person with computer access
  - Requirement 9: Restrict physical access to cardholder data
• Regularly Monitor and Test Networks
  
  o Requirement 10: Track and monitor all access to network resources and cardholder data
  
  o Requirement 11: Regularly test security systems and processes

• Maintain an Information Security Policy
  
  o Requirement 12: Maintain a policy that addresses information security

PCI DSS proof of compliance requirements vary according to the volume of transactions a business conducts. The chart below summarizes the four different Merchant Levels defined in the PCI standards:

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Validation Criteria</th>
<th>Validation Requirements</th>
</tr>
</thead>
</table>
| Level 1        | Any merchant processing over 6,000,000 Visa transactions per year or compromised in the past year, regardless of acceptance channel. | • Annual Report on Compliance completed by a QSA  
• Quarterly scans completed by an ASV |
| Level 2        | Any merchant processing 1 million to 6,000,000 Visa transactions per year regardless of acceptance channel. | • Annual self-assessment questionnaire  
• Quarterly scans completed by an ASV |
| Level 3        | Any merchant processing 20,000 to 1 million Visa e-commerce transactions per year. | • Annual self-assessment questionnaire  
• Quarterly scans completed by an ASV |
| Level 4        | Any merchant processing less than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 1 million Visa transactions per year. | • Annual self-assessment questionnaire and quarterly scans may be required as specified by the acquirer |

For more information on the PCI DSS requirements, please visit www.pcisecuritystandards.org.

Because PCI requirements cross all security sectors, no one vendor offers all of the technologies to satisfy every one of the PCI requirements. However, as virtually every institution that handles credit card data already has network firewalls, anti-virus, and in-transit encryption technologies deployed, compliance with the PCI standard is typically focused on deployment of application security and data protection mechanisms and the integration of defense-in-depth systems and policies.

Encryption: Protecting Data throughout Its Lifecycle

Most people are generally aware of encryption and the role it plays in data defense. But some myths about encryption still linger: the fear that encryption is impossible to manage in a distributed enterprise, will
slow network performance, will impact availability of data for use in critical business processes, or will result in irretrievable data if something goes wrong with the encryption scheme. Some of these ideas were valid decades ago when encryption technology was in its infancy, but all of these issues now can be managed with mature, modern encryption solutions backed by the right policies and procedures.

Modern enterprise class solutions are designed to make the best use possible of available computing cycles and will also take advantage of background processing to help ensure that encryption has virtually no impact on network performance or users. Loss of data if the encryption key is lost in a server crash or other incident can be successfully managed through proper key management, which would include a secure key recovery process.

There’s more than one way to encrypt data, but best practices and compliance regulations dictate that we use algorithms — different methods of scrambling data — that have been tested and approved by an agency such as National Institute of Standards and Technology (NIST). Solutions providers are experimenting with different ways of protecting data, some of which have not been approved yet. That’s great; we have to keep one step ahead of the malicious hackers, but a business that is using non-standard encryption to protect payment card data is out of compliance.

Encryption is typically packaged as a “solution” and includes tools to automate processes such as key management tasks. Annual rotation of encryption keys is required by data security regulations such as PCI DSS while security best practices indicate that rotation should be performed far more frequently. (The PCI Security Standards Council has indicated more frequent rotations will be required in a soon-to-be released revision of the standard). Look for solutions that provide an automated and secure mechanism — such as dual control of encryption keys, akin to a bank requiring two signatures before it will cash a particularly large check — for key rotation that requires little to no down time for the application.

Sometimes, of course, you have to unencrypt data in order to work with it. Access to payment card data should be carefully managed and granted only on a need-to-know basis which is typically managed by a role-based/policy-based access control technology. Policy-based access defines users’ (employees, contractors and agents) access rights and assigns unique access IDs and access privileges based on the organization’s security policies. Access rights are defined on an individual basis, or more efficiently through role assignment, and rights are limited to a specific period of time. For example, temporary workers or contractors are authorized access only for specific days and times during the work week or up to a specified date.
Another feature you may see in mature solutions is “centralized management of user access.” This allows the security administrator to change status of users and/or their access privileges from a single point of control and, with a push of a button, roll it out to all impacted databases. This is particularly useful when a breach is suspected, or the business has a large or frequent staff turnover.

**Understanding Tokenization**

Tokenization is a fairly new technology for protecting highly sensitive data. When you use tokenization the original data field is automatically removed from the data flow as early as possible and is replaced with a reference that points to the actual data field. Think of it as a claim check: you hand over your data to be stored in a secure location and you get a claim check. When you need the data again, you use the claim check to obtain the item in question, in this case sensitive data such as a credit card number. Happily there's no real claim check to worry about here, as the application processes everything behind the scenes.

In the event of a breach of the database or another business application, only the tokens could be accessed, which would be of no value to a would-be attacker. The actual payment card data is safe, stored in a highly secure server protected by robust encryption technology.

Tokenization allows enterprises to effortlessly reduce the overall risk that results from many persons having access to confidential data, often beyond what can be justified by business needs. And security is immediately strengthened by minimizing the number of potential targets for would-be attackers. Any business that collects, processes, or stores payment card data is likely to gain measurable benefits from tokenization.

Some merchants and service providers have refused to consider tokenization because it isn't yet specifically cited as an approved technology in PCI DSS. Those businesses that are implementing tokenization specifically for PCI often cite PCI DSS 3.1, which says to keep cardholder data storage to a minimum. Since tokenization reduces the number of instances of stored card data to only one instance, this seems justified. It’s certainly something to discuss within your own business and with PCI consultants.

One thing is certain though, tokenization does not take the entire point of sale out of scope. If the POS accepts credit or debit cards, then the POS is in scope no matter what. But when properly implemented, tokenization can reduce the PCI scope and make compliance more manageable. Some forms of tokenization can even take entire applications out of scope.
Delving into Data Masking

Data masking hides selected sections of a data field or record while allowing the rest of the information to be viewed by authorized users. This is a useful technology when a business needs to provide access to some parts of a customer record while protecting other parts. Properly masked data provides the information necessary for analysis, testing, and QA purposes without exposing the original, sensitive information. The masked data also retains its associations and referential integrity. The use of data masking in these scenarios enables businesses to significantly reduce their data security risk profile and is often required for regulatory compliance.

Traditional data masking solutions generate lower quality substitute data — random numbers, random digits, random dates, etc., constructed using building blocks called mask primitives — that are not adequate for some use cases. So many organizations are still quietly using unprotected sensitive data in the test system environment to avoid surprises when running the applications against real data in the production environment. This is a major security issue. Some organizations are addressing this problem by building a separate and fully secured environment for integration testing and system testing. This is a very costly approach and it will only solve the issue for the last steps in acceptance testing. In many cases this approach also creates a new environment with potentially new security issues.

If you decide to include data masking in your security implementation, look for a policy-based solution that creates masked data that is truly usable for test/analysis purposes. Be wary of solutions that provide limited options; a good enterprise solution should provide enough functionality to meet changing needs and changing regulatory compliance demands. In most cases you’ll want a solution that can be used with both operational databases in test environments and statistical databases (e.g., business intelligence, data warehouses).

Some people will insist that masking should never be reversible, and in many cases that may be true, but there are some situations in which you’d want a solution that is reversible, something that would make it possible to retrieve the original data. Other use cases can be supported by data masking using random data. And there are use cases that may require parts of the credit card or social security number to be accessible. You also want a solution that allows you to automate the process of generating data; otherwise the entire process will become too costly and time-consuming.
Tracking and Monitoring

PCI requires businesses to track and log all access to network resources and cardholder data. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

Data security solutions typically offer auditing tools. Mature solutions will track and log all attempts to access cardholder data, including the type of event, date, and time of event, and a success or failure indication. Audit logs obviously should be protected as well, access should be limited to authenticated persons with a job-related need, and that access will also be logged.

Database activity monitoring is a technology that’s been generating a lot of interest lately, but it’s important to remember that it should only be used in combination with other data protection technologies. Used properly, database activity monitoring is an appropriate solution for lower risk data. No encryption is involved here, the data is cleartext, and you are watching the data not making it unreadable. The point is not to shield that data but to provide increased visibility to how people are accessing and using an enterprise’s less-critical data. It’s a great supplemental tool in a comprehensive security plan.

In some cases we’re also seeing database activity monitoring used by businesses that are just beginning to roll out a comprehensive data security plan, or companies are using database activity monitoring alone to protect lower-risk data. It is a useful tool and a good complement to PCI-mandated protections, as long as you are aware that database activity monitoring is not a suitable way to protect high-risk data.

Policies and Processes

A critical component of PCI compliance is the implementation and on-going management of security policies across the enterprise. Policies define who has the rights to view, modify, destroy, or access cardholder and other sensitive data. To be effective, policies obviously need to be enforced, and applications have been developed to do just that.

A policy enforcement tool — or a data security solution that is policy-driven — automatically enforces an organization’s security policies across an entire enterprise. The best solutions come with pre-defined basic policies to make it easy for businesses to get the tool up and running, as well as allowing security administrators to customize the policies as needed.
A best-in-class policy management solution will include segregated security management and monitoring functions — these give organizations a way to completely separate security administration from data administration responsibilities, establishing a critical check-and-balance protocol.

**Beyond PCI**

Being in full compliance with PCI will result in a decent level of data security, and for some payment card processors that will be an improvement. But PCI was never intended to be an end point; it’s a foundation that was meant to be built on. Unfortunately the good intentions of PCI are lulling some payment card processors into a false sense of security, and the need to achieve compliance can siphon off time and budget that would be better spent deploying real data protection.

Take, for example, the recent case of the U.S. grocery chain that was certified PCI DSS compliant and yet was still wide open to an attack that exposed 4.2 million credit and debit card numbers. Apparently, malware installed on servers at more than 270 of the company's stores captured card data as it was transmitted from point of sale to payment card processors. The data was then forwarded to offshore servers. Had that data been encrypted, it's safe to assume that the subsequent 1,800+ reported fraud cases wouldn't have occurred, but since PCI doesn’t specifically require data to be encrypted at point of capture, the result was a PCI compliant merchant with a huge security hole that was just waiting to be exploited. (And if you were a savvy criminal, wouldn't you be looking just past those well-publicized PCI points of compliance for holes to exploit — such as data travelling unencrypted from cash registers?)

Security simply cannot be achieved by ticking off steps on a PCI checklist. Real security is holistic, encompassing technology, people, processes, and policies. It is hardwired into everything a company does, and is part of that company’s culture. And while it may seem like a real challenge at first to institute a comprehensive data security plan, ultimately a unified approach will be far more effective, increasing security and saving both time and money.

**********************************************************************************************************

**Sidebar: Common PCI DSS Compliance Mistakes**

The big compliance push isn't necessarily resulting in better data security. Compliance tends to encourage security-as-destination thinking — something that can be achieved and ticked off on the to-do list. But real security is an ever-evolving journey. Below are eight of the common mistakes enterprises make in their PCI compliance efforts — well-intentioned errors that often have a significant negative impact on budgets and data security, and the best practices that can help remediate these slip-ups.
Relying too heavily on quarterly scans for web application security assurance

The quarterly network scans mandated by PCI DSS 6.6 are a security checkpoint, not a method of managing web application security. Web applications are now a preferred attack vector for malicious hackers and as such need to be monitored on a continuous basis. For applications developed or customized in-house, the following “find, fix, prove” process must be continually performed: Identify vulnerabilities (find), correct them (fix), and test to confirm that the correction is effective (prove). Best practice also dictates that you secure the application level with a dedicated web application firewall, which helps organizations meet 8 of the 12 PCI DSS requirements.

Forgetting about the benefits of segmentation

In some cases, rather than re-architecting an entire enterprise environment and revising critical business processes across the board, it may be more effective from a cost and data security standpoint to move systems that collect, transmit, and store PCI-protected data into their own environment and restrict these systems interactions with the rest of the enterprise network. This allows the enterprise to focus its compliance efforts on the most critical components of the network.

Focusing too strongly on a single attack vector

Narrowing the enterprise’s focus to protect data against specific types of attacks often results in opening the doors to other types of attacks. Don’t implement a media-scare-story-driven security plan based on reacting to every overwrought report or bit of research. Constantly shifting focus to manage the threat of the moment will result in piecemeal security; focus instead on comprehensively securing data.

Focusing solely on complying with PCI DSS rather than implementing best security practices

Virtually all government and industry privacy and security regulations outline the most basic best practices of data security. Being able to pass a regulatory audit does not automatically ensure effective security. Instead of trying to protect your organization’s data assets by solely striving to meet individual regulatory requirements, focus on acting in accordance with data security–centred best practices, reinforced by security solutions such as automated policy enforcement, encryption, role-based access, and system auditing. In other words, do the right things instead of just the required things.

Assuming that PCI responsibility can be outsourced

If a business is required to comply with data protection standards or regulations, and its outsourcing partner fails to protect that personal data, the company that owns the data will most likely be considered at fault and liable for any associated costs, penalties, or legal actions that might arise from its exposure. You must ensure that the company you are partnering with — offshore or domestic — takes data security seriously and fully understands the regulations that affect your business.

Allowing PCI to become a series of projects
Disparate data protection projects, whether created by design or due to company mergers, often result in an impossible-to-manage hodge-podge of secured and unsecured systems, with some data on some systems encrypted and some not, some systems regularly purged of old data on a monthly basis and others harboring customer information that should have been deleted years ago. If this is the case within your enterprise, consider appointing one person as the PCI DSS compliance manager, to serve as a single point of contact and authority for compliance efforts and, ultimately, to develop and deploy an enterprise-wide unified plan to manage sensitive data assets and enable compliance with applicable regulations and standards.

**Assuming an enterprise can build on PCI security investments into infinity**

The success of an enterprise's security efforts need to be regularly reviewed and measured; older goals may need to be dropped, new plans may need to be instituted, and sometimes technologies that seemed like great ideas at the time may become a gaping security hole as a result of new discoveries. DES encryption, for example, was once considered secure until researchers proved it was vulnerable to brute force attacks due to its short (56-bit) key. Security is always a moving target and we have to be willing to move forward as conditions demand.

**Ignoring the corporate culture**

Security measures that aren't understood and fully embraced across the enterprise can and will be circumvented. As you plan and implement PCI DSS, don't stint on ensuring that employees understand the importance of keeping customer data secure and protected and have the tools and training they need in order to secure that data.
Banking the Unbanked Using Prepaid Platforms and Mobile Telephones in the U.S.

Francesc Prior Sanz† and Javier Santomá§

Introduction

The rapid growth of mobile phone usage and the continuous rise in wireless coverage fuel the expectations that access to financial services through mobile phones could transform the way financial services are provided. The emergence of new and more efficient business models can potentially resolve supply inefficiencies that explain the large unbanked population that exists in the U.S., much larger than in most developed countries.

Nearly 40 million U.S. households (approximately 73 million people) are financially underserved, of which 15 million households (approximately 28 million people) are totally unbanked. This problem is explained by the inadequacy of the value proposals offered by financial institutions to the demands of the U.S. customers. The areas of poor alignment refer mostly to the design of products and the marketing and distribution networks used. To resolve these misalignments, this paper will argue that business models based on prepaid cards as products and mobile phones as transactional and distribution channels could be used in order to close the supply gap. We will call the business model proposed based on prepaid products and mobile phones mobile banking, since these two elements are the basis of the business model used by companies such as Smart Money and G-Cash in the Philippines, Wizzit in South Africa, and M-Pesa in Kenya.

† Francesc Prior Sanz has extensive international experience both in academia and in the financial services industry. In academia, he currently serves as Research Associate at IESE Business School (Barcelona) and as Associate Professor of Banking and International Finance at Universitat Internacional de Catalunya (Barcelona). From 2005 to 2008, he was Director of the Financial Inclusiveness Program at Florida International University (Miami). He has also taught microfinance courses at Universidad Metropolitana de México (Mexico) and Escuela de Ingenieros Julio Garavito (Bogotá).

§ Dr. Javier Santomá is Professor in the Financial Management Department at IESE Business School. His areas of specialization include portfolio management, company finance, insurance and finance for new companies. Dr. Santomá received his Ph. D. in Managerial Science and Applied Economics from Wharton School of Business at the University of Pennsylvania.
The involvement of banks and telecom operators in the delivery of financial services through mobile phones creates, according to the Mobey Forum,¹ four different mobile financial services ecosystems. David Porteous added to this analysis the distinction between four critical roles played in each scenario by the bank or the telecom operator.² He argued that the first role to consider is who is legally responsible for the deposits; the second is who bears the reputational risk (implying whose brand is more exposed to the public); the third is whether deposits can be accessed through agents or only through bank branches or ATMs; and the fourth and final role considered is who carries the payment instruction. Based on this framework, the four business models defined by the Mobey Forum have the following characteristics:

### Table 1: Classification of Emerging m-Banking Models³

<table>
<thead>
<tr>
<th>Model name</th>
<th>Bank-centric models</th>
<th>Collaborative models</th>
<th>Independent service providers</th>
<th>Operator-centric models</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-Who holds accounts/deposits?</td>
<td>Bank</td>
<td>Bank</td>
<td>Bank</td>
<td>Telco/ Non bank</td>
</tr>
<tr>
<td>2-Whose brand is dominant?</td>
<td>Bank</td>
<td>Joint- Non Bank or Telco</td>
<td>Usually non bank or telco dominant</td>
<td>Telco/ Non bank</td>
</tr>
<tr>
<td>3-Where can cash be accessed?</td>
<td>Bank</td>
<td>Any telco (sometimes 3rd party payment gateway)</td>
<td>Usually specific to one telco</td>
<td>Telco network + other</td>
</tr>
<tr>
<td>4-Who carries the payment instruction?</td>
<td>Additive models</td>
<td>Smart/ MTN</td>
<td>Wizzit/ G-Cash/ MPesa</td>
<td></td>
</tr>
</tbody>
</table>

According to this classification, the “bank-centric model” implies only developing new channels for existing banking products. Porteous calls this model “additive” and argues that this type of business model does not transform the way financial services are provided. The three remaining business models, however, do transform them and therefore we call them “transformational models” since these business models based on prepaid electronic payments systems and cellular technology address the supply inefficiencies in the distribution of financial services.

The use of transformational mobile banking business models could be the catalyst for change in the way financial services are provided to the less affluent. This paper will analyze how “transformational business models” of mobile banking based on prepaid platforms that have been implemented in developing nations

---

² David Porteous, “The Enabling Environment for Mobile Banking in Africa,” (report produced for the DFID, 2006).
³ Ibid.
can be used in the U.S. to provide financial services to the underbanked. Indeed, the emergence of card and prepaid systems in particular, coupled with the use of cellular technology, could to transform the way financial services can be provided. The cases of Smart Money in the Philippines (a partnership between a telco and a bank), Wizzit in South Africa (an independent service provider), and G-Cash also from the Philippines (as an example of an operator-centric business model), show how these business models have been successfully used for banking the poor in developing nations.

Transformational mobile banking business models have not developed extensively in developed nations. NTT DoCoMo in Japan has been the only successful transformational model of mobile financial services in Europe, Japan, and the U.S. In Europe, the initiatives of Paybox AG (Germany) and Mobipay SA (Spain) ended unsuccessfully. Paybox is an independent service provider that was about to become the industry standard in 2002, but the failing of its strategic alliances lead the company to its final unsuccessful fate. Mobipay followed a collaborative model between financial institutions, mobile telecom operators, and payment processors. Demand did not pick up, however, and its operations have remained very limited in scale.

The reasons why mobile banking has not taken off in Europe are twofold: first, the lack of demand due to the slower development of e-commerce and a much higher level of banking access, especially among immigrants; and second, the unclear regulatory framework that creates regulatory uncertainty for mobile operators that want to implement transformational models and a competitive disadvantage position for independent service providers (such as Wizzit in South Africa). As a result, we find that mobile banking models in Europe are mostly “additive,” implemented by existing banks that use mobile phones as an additional channel in the context of multichannel strategies. Moreover, the slow development of ELMIs (nonbank issuers of e-money) and the prepaid industry in Europe—mostly due to the lack of demand but also to some regulatory problems regarding electronic vouchers (gift cards, meal cards), transport systems, and travellers cards—gives potentially interested mobile operators no technology platform to operate with other than banks. As a result, and given the current legal loophole regarding mobile operators, they prefer to operate within a close network (allowing customers to buy ring tones and digital content) instead of developing alternative business models such as G-Cash in the Philippines.

Japan and Korea are the only developed countries where mobile banking has been a real business success. Japan’s mobile banking market is quite unique in several aspects, due to the dominance of NTT DoCoMo. DoCoMo’s successful mobile banking strategy is based on building the supply side of the market by offering attractive commercial terms to banks, card companies, transport companies, merchants, and consumers by
subsidizing their handsets. Of particular relevance in the success story of NTT DoCoMo is the development of the Felica technology of near field communications with Sony. Indeed, the success story of NTT DoCoMo shows the success of an operator-centric model.

In the U.S., transformational models of mobile banking have not developed extensively either, due mostly to the structure of the telecommunications industry in the country and to the lack of standardization in a fractured wireless market. However, the recent and important development of the prepaid industry could be the catalyst for a service that has potential demand (the unbanked population in the U.S.—especially immigrants), and where no major regulatory obstacles exist.

This paper will begin describing the way card and prepaid systems work, since we argue that development of the prepaid industry in the U.S. could be the catalyst for the development of mobile banking in the country. Indeed, as it will be subsequently shown when we review the development of the prepaid industry in the U.S., the emergence of new players aiming at serving the underbanked gives mobile operators the possibility of partnering with prepaid cards issuers and transforming the way financial services are provided to the poor.

The Emergence of Prepaid Card Systems: How Do They Work?

The increase usage of card systems has been the driving force behind the development of prepaid cards systems in the U.S. Cards can be used for basic payment functions such as cash withdrawals at ATMs and EFTPOS (electronic funds transfer points of sale), where cash back is offered, and purchases at retailers with EFTPOS. EFTPOS can be physically located at a store where the payment is made, or located in a remote location (virtual EFTPOS). Virtual EFTPOS allow for additional payment functions such as bill payment, internet purchases, or direct debits. However, depositing cash in a card (cash in function) is limited to stored value (prepaid) cards, and depends on the regulation of both stored value cards and e-money.

Card payment systems can be classified according to the way transactions are authorized and authenticated. The first classification is whether the transaction is authorized using a line of credit, the actual value of deposits in the bank account (debit), or the amount of e-money in an internal account (prepaid). The second is whether the transaction is only authorized when the acceptance network is online or also when the system is offline. The third is whether the transaction is authenticated by inserting the personal identification number (PIN) or by signing the receipt (either physically or electronically).
Table 2: Types of Card Products Based on Authorization and Authentication Mechanisms

<table>
<thead>
<tr>
<th>Credit</th>
<th>Bank account balance</th>
<th>Internal account</th>
<th>Online</th>
<th>Offline PIN based</th>
<th>Signature based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepaid</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Only if PIN based</td>
<td>If POS not enabled</td>
</tr>
<tr>
<td>Debit online</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>For very limited transaction amounts</td>
<td>If POS not enabled</td>
</tr>
<tr>
<td>Debit Offline</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>If POS enabled, always in ATM's</td>
<td>Yes</td>
</tr>
<tr>
<td>Credit</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td>If POS enabled, always in ATM's</td>
<td>Yes</td>
</tr>
</tbody>
</table>

These three characteristics determine the types of cards currently available and their payment functions. Credit cards were the first type of cards issued in the U.S. This product allows credit card holders to buy products or services at retailers with EFTPOS for an amount less or equal to its credit limit. Additionally, this type of card can be used when the EFTPOS is offline, as long as the transaction does not exceed the value determined for this type of transaction (this maximum value or back-up parameter is usually large enough to allow for the necessary expenses when the customer has no access to an EFTPOS online). The authentication mechanism for credit card transactions at EFTPOS has traditionally been signature based. However, in some countries such as France and recently worldwide due to the EMV initiative, EFTPOS does or will require authentication using the PIN number. The authentication mechanism for credit card transactions at ATMs is PIN based. Cash back at EFTPOS is not currently available for credit cards in the U.S.

Online debit cards were issued later by financial institutions mostly in Western Europe and other regions of the world. In the U.S. its deployment has been slower, due to the importance of offline debit, although this is changing progressively. Online debit cards were originally marketed as ATM cards, to allow cardholders withdraw money from their bank accounts. As a result, every debit card transaction has to be authorized verifying online the monetary value of the bank account linked to the debit card. Transactions will be accepted if the amount of the transaction is not higher than the monetary value of the bank account (in some cases including its overdraft limit). Debit cards are also currently being used to buy products or services at retailers with EFTPOS, although for those transactions to be approved, the EFTPOS has to be connected online through its switch to the core banking platform of the issuer. If it is not online, some issuers in some countries give some back-up parameters to allow microtransactions while the EFTPOS is
offline (less than 50 Euros⁴). In the U.S., the authentication mechanism used for online debit is PIN based, which allows the cash back function to be more widely developed. In other areas of the world, however, online debit authentication is signature based, which does not support the development of the cash back function.

Offline debit is a product mostly developed in the U.S. and it is still the predominant type of debit card in this country.⁵ However, due to the legal process launched by Walmart in 2003,⁶ its importance has decreased considerably over the past years. Its main difference with online debit is that the type of EFTPOS that accept this product are not connected through its switch to the core banking system of the issuing bank, but instead are connected to the credit payment networks of Visa and Mastercard. As a result, the authorization mechanism used verifies the credit limit that both payment networks have informed in their authorization databases. This credit limit is calculated every few days based on the information provided by the issuer in terms of the monetary value of the banking account of the cardholder linked to this debit card. However, it does not reflect the exact value online, and therefore generates overdraft risk for the issuing institution if the cardholder spends more than the monetary value of the bank account. The rest of offline debit features are similar to credit cards, since both products are marketed and accepted by the same payment networks. In summary, offline debit cards are credit cards (they have credit card BINS⁷), but are payable the following day by the cardholder (or the number of days that the system takes to settle the transactions).

Stored value cards or prepaid cards are the last type of cards launched to the market by card issuers. This product allows cardholders the same payment functions as online debit, but the main difference is that the transactions are not authorized verifying the monetary value of the bank account linked to the debit card, but instead the authorization process is based on the monetary value of the internal account that the prepaid card is linked to. This monetary value is gathered in a database that manages this type of internal or prepaid account. The legal definition of prepaid accounts is one of the most important topics that this analysis will cover as well as the additional functions that these types of accounts could have if the appropriate regulatory framework was applied. The ultimate goal of this study is to analyze how stored value cards could be used to collect deposits in a payments architecture where any EFTPOS, ATM, or any

⁴ See Porteous, “Enabling Environment,” (amount defined as the limit for microtransactions).


⁷ Card identification numbers.
other terminal connected online to the payments systems could perform this function for any given issuer. However, a basic understanding of how prepaid systems currently work is required in order to achieve this goal. The following description briefly presents the way prepaid systems currently operate.

When a consumer buys a product or a service using a prepaid card from a merchant, either at a physical store (physical EFTPOS) or from an online retailer (virtual EFTPOS), the customer swipes or inserts the card in a physical EFTPOS, or inserts the card number in a virtual EFTPOS online. The EFTPOS establishes a secure protected connection (secure sockets layer, or SSL) with the server of the prepaid service provider (PSP). The server authenticates the customer either by using a PIN or by using his signature—physical or electronic—and checks the amount of funds available in the prepaid account (value of the prepaid account) in order to approve the transaction. The PSP sends the information to the merchant regarding whether the transaction has been approved or declined, and if it is approved the PSP credits the account of the merchant (only for accounting purposes) and debits the account of the consumer. Once the transaction is approved, the merchant confirms the purchase and provides delivery details if the transaction is online.

At the end of the day, the merchant sends the PSP the total amount of transactions approved, and the PSP settles the payments the following day (or the number of days agreed in the contract) by crediting its bank account. The settlement account of the merchant cannot be its prepaid account since the regulator (when the regulator regulates e-money or prepaid accounts) establishes purse limits that are usually too small for merchants. The consumer can load his prepaid account using a variety of systems that depend on the local legislation of e-money. Usually, prepaid accounts can be loaded online or by phone, at a participating retailer, or at the branches of the PSP if it has any. Prepaid accounts allow also the consumer to withdraw cash at any ATM connected to the system, at a POS connected to the system with cash back function, or at any participating retailer or branch of the PSP.

Prepaid platforms have characteristics that make them especially useful for developing low cost payments systems:

1) Customers using prepaid systems do not need bank accounts, debit cards, or credit cards

2) Users do not need to develop or invest in new technologies

3) This payment mechanism can be used in a number of platforms such as PCs, mobile phones, handheld and set-top boxes

4) It is a payment system specially designed for micropayments, microdeposits, and even microcredits
5) Allows users to control their cash flow by receiving statements (either online or physically, depending on provider) or accessing balances through PCs, mobile phones, hand-held and set-top boxes.

**Figure 1: Processing POS Payments Using the Prepaid System**

Prepaid cards use accounts to manage funds in real time through host computer systems. The accounts are held in a single concentrator account with different subaccounts for each card. Some are “pooled” accounts and some, for accounting purposes, are actual bank accounts held by the individual consumer, depending on how the issuing financial institution treats the accounts. These cards have regular debit or credit card POS and ATM functionality. However, prepaid cards have the additional feature of being reloadable in a variety of ways at a range of locations. That is why the functionality of prepaid cards closely resembles that of traditional bank accounts, and therefore why they are the basis of the model proposed.

A few recent papers have examined the role of the prepaid industry serving the unbanked and underbanked markets in the U.S. Frumkin, Reeves, and Wides of the Office of the Comptroller of the Currency identified payroll cards that can be used for the direct deposit of paychecks, without a necessary link to a bank account as an innovative product for reaching unbanked and underbanked markets and conducted a survey of financial institutions in the payroll card market. However, banks have not taken an active role in the market. They are still studying and trying to understand how payroll cards can be sufficiently profitable, by exploiting cross-selling opportunities with the unbanked.

---

8 See Prior Sanz and Santomá, 2008.

The possibility of using prepaid cards for asset- and credit-building purposes was raised by Chakravorti and V. Seidman in a paper discussing the convergence of the interests of the financial services sector and low-income consumers. Chakravorti and V. Seidman pointed out the growing prevalence of prepaid cards in low-income markets and the need for greater consumer protections and functionality for these cards in order for them to truly mimic bank accounts.

Prepaid cards could be a valuable financial tool for the unbanked population in the U.S. for several reasons. First, prepaid cards generally lack the identification and credit requirements that effectively bar millions of individuals from opening traditional bank accounts. Second, prepaid cards can be purchased and reloaded at a growing number of locations other than bank branches, such as check cashers, convenience stores, and other retailers. The ability to load cards in multiple fashions at a variety of locations is the key to success for these products and therefore retail distributions are key to prepaid providers. This is why they are pursuing partnerships with money-service businesses, convenience stores, and other retail distribution channels to increase prepaid users’ reloading options. Third, prepaid cards can provide immediate availability of funds at a cost that is, in some cases, lower than some other alternatives for unbanked consumers. Fourth, prepaid cards are difficult to overdraft, reducing the likelihood of unexpected fees. Fifth, many prepaid products offer some sort of bill pay option, especially branded cards that enable signature-based transactions. Since many prepaid users are unbanked, the functionality of paying bills without using checking accounts or money orders is important. However, most bill pay options for prepaid card users are online or in-person. Additional physical options are required, such as self-service bill pay at kiosks in retail locations, that could provide additional functionality for unbanked consumers.

Six, a significant number of prepaid cards providers offer remittances. This feature allows U.S. cardholders to transfer funds to authorized family members in other countries. Prepaid-based remittance features are structured in at least two ways. Sometimes, dual cards are issued to customers, and one of the cards is sent to family in another country to access funds from the sender’s “account” via ATMs. Other cards allow cardholders to designate “subaccount” holders in other countries for the purposes of transferring money. In these cases, the subaccount holder has access only to the money that the primary account holder designates to share.

---


12 Barr, Banking the Poor.
Review of the Prepaid Card Industry in the U.S.

Prepaid card systems in the U.S. operate in two ways. One is the “closed-loop” system, which is the largest component of the prepaid card market. Closed loop prepaid cards can only be used for the issuers’ products or for limited purposes, such as prepaid gift cards at retailers like Borders or Starbucks in a closed payment network. The issuer and the merchant are therefore the same entity. The second one is the “open-loop” system that offers consumers the ability to utilize their cards for multiple purposes, such as making purchases at a variety of stores or paying bills. These cards are accepted in payment networks open to multiple issuers, where merchants and issuers are different institutions. This open payment infrastructure is the basis of bank card systems and therefore currently used for debit and credit cards.

Closed-loop prepaid systems were first introduced in the early 1990s and open-loop cards became available by the middle of that decade. Closed-loop systems were originally used as a payment instrument in retail stores (sometimes provided as a gift card), but are also extensively being used as a payment instrument in transport systems and mobile telecommunications. Originally, retailers and department stores developed this kind of system in order to avoid paying discount fees to merchant banks. Closed-loop systems do not belong to payment networks and as a result are also called “non-branded cards.”

Open-loop prepaid cards offer consumers the ability to use their cards for multiple purposes in multiple locations. Open loop prepaid cards are therefore the equivalent of online debit cards for unbanked customers. Open-loop cards are accepted in open branded networks such as Visa or Mastercard and therefore are called “branded cards.” MasterCard, Visa, American Express, or Discover branded cards use both signature-based or PIN-based authentication mechanisms. MasterCard and Visa branded prepaid currently dominate the market, but Discover and American Express branded-prepaid are becoming widely available as well in the U.S. Their competitive position might also strengthen in light of recent antitrust lawsuits levied against Visa and MasterCard. Discover, for example, purchased Pulse EFT Association, an Electronic Funds Transfer (EFT) network with over 4,000 financial institution members. This could have further implications on future branding for prepaid.

Open-loop systems can be grouped into three categories: first, payroll-only cards, which can be used only for direct deposit of paychecks or, in some cases, for receiving other automated clearinghouse (ACH) transactions. Open-loop cards can also be used for pre-authorized payments, such as rent or utilities. Finally, open-loop cards can be used as a general-purpose payment instrument, such as a prepaid debit card.

---

13 These kind of closed systems are also called private networks.
14 Discount rates are paid to banks by retailers, when customers use bank issued cards to pay for goods at a EFTPOS.
15 Branded networks such as Mastercard and Visa.
deposits such as Social Security Payments; second, reloadable payroll cards, which serve primarily as direct deposit cards for payroll checks but offer consumers other ways to reload the cards; and third, general purpose reloadable debit cards, which consumers can reload in a variety of ways at a range of locations.

Payroll-only cards were thought to be one of the most promising types of prepaid products. However, they are generally only used for direct deposit of paychecks and other automated clearinghouse (ACH) deposits, such as Social Security or disability payments. Typically, prepaid providers market payroll cards directly to employers, who then distribute the cards to their employees. Most prepaid cards do not currently work in a way that allows a single card to contain all levels of functionality—payroll, general spending, etc. Consumers who have payroll cards, for example, may not be able to or may not be aware that they are able to load other deposits besides payroll deposits onto their cards.

Many payroll cards are only set up to accept streams of direct deposits; manual reloads might not be available. However, some providers offer reloadable payroll cards. Integrating different types of prepaid cards and adding functionality, such as reloadability, payroll direct deposit, bill payment, and so forth are important innovations for the future of the prepaid industry if it wants to provide an attractive value proposition to consumers.

The major players in the U.S. prepaid card market today are nonbank providers of reloadable prepaid debit cards such as Green dot, NetSpend, and Next Estate. Banks are also providers and issuers of prepaid cards such as Bankfirst, Bank of America, Citibank, and J P Morgan Chase; prepaid processors such as Metavante, StarSystems, WildCard, and Galileo; providers of back-end services for prepaid cards, including ATM and POS processors; and payroll firms such as Paychex and Comdata. The distinction between products that are distributed by financial institutions and those distributed by nonbank firms is an important one. Products distributed by banks and credit unions are more likely to have additional consumer protections, lower pricing (because fewer actors are involved), and more obvious transitions into other financial products and services.

Prepaid cards offer interesting opportunities for banks that see low-balance savings accounts as cost-prohibitive products. If the prepaid industry can figure out a way to offer savings and other benefits to previously unbanked consumers, it would be a win-win proposition for customers and companies alike. As issuers, banks hold the funds underlying prepaid cards in a variety of ways. Some banks hold the funds off-balance-sheet, in fiduciary accounts. Others hold the funds on the balance sheet in pooled accounts, perhaps in the name of the card’s distributor, or in the case of payroll cards, in the employer’s name; while still others provide individual deposit accounts in the name of each cardholder.
For large banks, interest in prepaid products may be partly due to their greater involvement in the payroll card market than in the general spending market. Prepaid cards are therefore sold to employers, who offer the cards to employees providing consumer protections similar to those enjoyed by traditional bank accountholders. Payroll cards give banks data about customers that could then be used for opportunities in cross-selling other bank products.

On the other hand, certain small regional banks, such as the Central Bank of Kansas City and University Bank in St. Paul, have created new prepaid programs that are intended to serve as entry-level products for consumers who might access additional bank services in the future. In another recent development, New York Community Bank, the fourth largest thrift in the country, has begun to offer prepaid cards in its branches. The Bank is marketing the cards as entry-level products, and is also marketing to customers who are denied checking accounts or who prefer prepaid instruments.

Nonbank firms are beginning to replace bank distributors as the most active actors in figuring out how to add enhanced features to prepaid products that could provide increased service to lower-income consumers as the marketplace matures. Perhaps because of regulatory uncertainty, to be discussed later, or a more conservative approach to entering new markets, banks are lagging in innovation with regard to these products.

The most important remaining challenge for prepaid issuers, however, is to figure out a business model that assures profitability. Issuers do not currently know what features make products successful. However some facts are clear: first, large scale is needed to be profitable. Second, in order to develop a profitable prepaid business model, customer relationship management strategies using data mining processes are required. These processes are already widely used in the credit card industry and therefore the synergies between credit card issuers and prepaid issuers need to be exploited. Providers of prepaid cards need to take into account how many cards are active in their system, how much money is loaded onto each card, how frequently the cards are used, the number of transactions occurring each month, and how much unspent money is left on unused cards.

Prepaid cards’ main income streams are fees paid by cardholders for activation, maintenance, and debit transactions, as well as through interchange fees from merchants and earnings from float on the funds held. The lack of consensus around the key profitability drivers might help explain the wide variety of pricing structures and fees levied by prepaid providers. The business case has not been clearly defined and issuers of prepaid cards are unclear on what specifically attracts consumers to stored value products.
Although the increasing competition in the marketplace is decreasing prices for prepaid cards, they are still higher than regular bank accounts. The fees that consumers might pay to sign up for and use prepaid cards are estimated for general purpose cards at $25.45 a month. Costs of a regular bank account are smaller. Bankrate.com conducted a survey of checking accounts in spring 2003 and discovered that the average monthly fee for a non-interest bearing checking account in the country’s 25 largest markets was about $6. Therefore, a prepaid card could be a highly expensive option, perhaps even more costly than using a check casher for basic transactions. In other cases, however, a prepaid card with a lower pricing structure or a structure that is consistent with the holder’s usage pattern could be cheaper for certain consumers than using a check casher.

Prices could come down if additional income revenues were exploited. One potential feature that is currently lacking in most prepaid cards is the ability for cardholders to save and build assets. Families with relatively low incomes have assets that could be stored in a savings vehicle. But many of these families may not have access to traditional accounts at banks or credit unions. Therefore, demand for savings features in prepaid products is potentially powerful.

Research shows that lower-income consumers desire products that provide a safe, convenient, and inexpensive way to pay bills, make purchases, save, and build credit. For example, a 2000 industry survey of check-cashing customers showed that 49% would use savings accounts if they were available from their regular check-cashing outlets. Market research in lower-income urban markets showed how an overwhelming majority of low and moderate-income consumers, given the opportunity to spend $10,000, would invest the money in some type of asset-building opportunity. But in order to save, lower-income families need 1) an opportunity—or the ability—to access a savings vehicle; 2) incentive, or the ability to earn interest on funds; and 3) motivation, such as direct deposit, which makes automatic saving much easier.

---

18 The Federal Reserve Board’s 1998 Survey of Consumer Finances estimated that 60% of households at or below the poverty level had positive assets.
A few prepaid companies have experimented with offering savings features with their cards. Directo included a savings component as part of the bundled services offered with its card program, but the company suspended it in part because few customers were using the feature. NetSpend, one of the largest providers of prepaid cards in the U.S., launched a strategy to link a savings vehicle with its prepaid program. IndiGOCARD started a program linking savings accounts to its prepaid program but has marketed it as an overdraft protection program. Linkages with savings accounts, tax refunds (such as the prepaid programs offered by Jackson Hewitt and H&R Block), Individual Development Accounts (IDAs), or other savings vehicles through an issuing financial institution are possibilities for prepaid cards’ growth.

However, prepaid card providers must face important customer barriers to providing unbanked consumers with savings opportunities. First, savings or credit-building features would require more stringent identification verification. This requirement would decrease the relative anonymity offered by prepaid cards, which is one of its most desired features. Second, prepaid users may not want transaction history data to be reported for credit-building purposes. They may wrongly perceive that such data could negatively affect their credit scores, based on their previous banking experiences. Third, “saving” has different meanings for different people and therefore the product may need to be adapted according to the type of customer targeted. For some, a rebate or a flexible spending account may act as a savings feature. For others, “savings” vehicles must provide accessibility, tangibility, anonymity, or other concerns.

One of the most important perceived customer barriers to providing unbanked consumers with savings opportunities through prepaid cards is the lack of consumer education in the appropriate use of such features. Consumers already face difficulties in understanding how prepaid cards work, how fees are structured, and how to manage their funds. To solve this problem, employees at current prepaid cards distribution points (places of employment, check cashers, retail locations) should be more willing and able to explain products to consumers. As a result, adding new features such as savings and credit-building features may require a level of sophistication and education in consumers that does not currently exist.

A second potential revenue source for prepaid card issuers could include adding credit-building features to their products. Since cards are marketed primarily to unbanked customers, prepaid cards have the potential to be an effective personal financial management tool for some people. However, very few companies are attempting to provide credit-building features such as a payday advance or overdraft protection feature tied to a prepaid card.

These small extensions of credit, both formal (such as payday advances) and informal (such as paying overdrafts on a discretionary basis) could be an additional feature that would add value to the issuer’s
prepaid value proposition. However, even if these products were marketed rightly they would not
currently help build a consumer’s credit score. Existing credit models do not allow for the reporting of
credit relationships lasting fewer than 30 days.\textsuperscript{21} IndiGOCARD, Eufora Credit Builder, and NetSpend
CredAbility programs tried to utilize the credit-building component as a marketing tool for the cards,
extensively advertising this feature and using a variety of strategies to try to link prepaid with the credit
bureaus.

The structure of the United States’ credit reporting system presents therefore important barriers for the
development of credit features tied to prepaid. First, currently the credit bureaus do not accept individual
tax identification numbers (ITINs) as an identification document, although the U.S. Patriot Act allows for
the acceptance of ITINs as a substitute for Social Security numbers for credit reporting purposes. Second,
credit bureaus currently can only collect credit data; debit and prepaid data are not considered to be
“credit.” Some prepaid companies have attempted to report monthly fees as “bill payments.” However, laws
in some states restrict the reporting of bill payment histories by utility companies, although the federal
Gramm-Leach Bliley Act (GLBA) allows such reporting by financial institutions to credit reporting agencies.
As a result, current credit-scoring models in the U.S. do not use prepaid-related data.

International experiences in credit scoring models prove that prepaid usage information should be used. In
many European countries, the practice of collecting deposit data for scoring purposes is widespread, but
the data is usually limited to the internal system of the financial institution (banks cannot view another
institution’s customer data). Some have argued that the Fair Credit Reporting Act (FCRA) has prevented
financial institutions and other entities to report prepaid transaction information due to privacy issues.\textsuperscript{22}
However, as long as institutions follow FCRA guidelines, privacy issues should not stop banks and others
from reporting prepaid transaction data to the bureaus. Nonetheless, this is not presently occurring in the
marketplace.

Adding credit features to prepaid cards can also generate other regulatory problems. It is unclear whether
these services should be considered extensions of credit from a regulatory perspective and therefore
subject to corresponding disclosures and regulations. Besides, the ultimate benefit to the consumer is
disputed, since the costs of payday lending and overdraft protection are so high. Some argue that low-

\textsuperscript{21} Fair Isaac Corporation recently announced the development of a new credit score for those with little or no credit
histories; this credit score may use data on payday loan repayment, although it is unclear how such data would be
used.

\textsuperscript{22} For example, how much money went into an account, and how much came out, in addition to information on
balances and length of card ownership.
income consumers should be able to access small credit at reasonable costs, and that currently these costs are prohibitive.  

**Mobile Banking in the United States**

In the U.S. approximately 17.5 million people with mobile phones do not have access to bank accounts. Mobile banking services in the U.S. could be highly attractive for this group, taking advantage of the synergies with the existing value propositions being offered by issuers of prepaid cards. The success of mobile banking with this part of the population will depend on whether the value proposition is right in terms of prices, distribution method, usability, security, product design, communication, and marketing. However, the high adoption rates of new mobile technologies by the demographic groups most likely to be underbanked fit well the eventual acceptance of MFS, if appropriate value propositions are offered.

Mobile banking services have not had the same degree of technological innovation and market penetration in the U.S. as in other international markets such as Japan or the Phillipines. The most important obstacle to the development of mobile banking in the U.S. is the structure of the telecommunications industry in the country. The slow standardization and the fractured wireless market impede the take-up of mobile banking in the U.S. Mobile phones' penetration in the U.S. is lower than in most developed countries, and even lower than in some developing nations. High penetration in some developing countries can be traced to the lack of legacy land-line infrastructure. As a result, users have moved directly into wireless telephony.

The continued lack of dependable, universal wireless coverage, even in metropolitan areas, renders mobile banking alternatives like online banking more reliable and user-friendly. And because the United States mobile market is only now approaching saturation, carriers have remained more focused on customer acquisition than on increasing functionality, prioritizing “new subscribers over new services.” Finally, some experts suggest that consumers in the United States may be less willing to engage new technology than in other markets as Korea and Japan.

From a regulatory perspective, federal and state banking regulations may limit the financial services that telecommunications companies can provide. As a result, carriers may be obliged to partner with banks or third-party providers, slowing the development of MFS solutions lead by telecoms. However, the recent and important development of the prepaid industry could be the catalyst for a service that has potential demand since the unbanked population in the U.S.—especially among Hispanic immigrants—is very

---

23 Center for Responsible Lending, Presentation at the IFC Building, October 2007.
relevant. Telecommunication companies could partner with specialized providers of prepaid cards in serving the unbanked, and therefore increasing accessibility and functionality to existing prepaid cards. Regulatory issues should not be a concern, since prepaid cards are already regulated as Money Service Businesses (MSB), and telecoms could be viewed as agents currently not regulated under the MSB framework.

Beyond the specific challenges that will be encountered by individual players, a number of general questions face the emerging mobile banking industry in the U.S. First, security and how providers can balance convenience and security to ensure that both users and providers are fully protected against fraud, data theft, and other threats. Second, reliability and how the mobile financial services infrastructure can prove dependable enough to attract and retain customers. Third, partnership models and what kinds of revenue-sharing arrangements will accommodate key players without proving prohibitively expensive for end users. Under these agreements, the key element of discussion will be to determine who “owns” the end-user relationship. Fourth, achieving necessary volume and network effect issues, by convincing not only consumers but also merchants and distribution networks to build a sustainable business case. Fifth, to what degree legacy systems will be an obstacle for the development of new mobile banking solutions.

**Emerging domestic players**

Established banks such as Citigroup (Citimobile), J P Morgan Chase, HSBC, and Bank of America have developed “additive mobile banking business models” where transactional services are offered by mobile telephone on traditional banking products.\(^{25}\) The most advanced multichannel offering using mobile phones, however, has been the mobile banking offering from Banco Popular. The bank, which has branches in six U.S. states and throughout the Caribbean, allows users to consult their account balances by text message and sign up to receive notifications for various types of account activity. The free service is currently available to users of Centennial Puerto Rico, Cingular, Movistar, and Verizon.

Among domestic mobile carriers, Cingular, currently being rebranded as AT&T, is leading the market as it announced its mobile banking alliance with enabler Firethorn Holdings, a mobile transaction streamlining company. However, its mobile banking strategy has been limited to providing an additional transaction channel to established banks, and therefore allowing them to implement additive mobile banking business models. In March 2007, AT&T signed a partnership with Wachovia Corp. and other banks that will allow subscribers of its Cingular brand to check account balances, transfer funds, and receive or pay bills. The

\(^{25}\) Porteous, “Enabling Environment.”
Firethorn technology connects with Firethorn’s servers, which then communicate with the users’ bank systems.

Among manufacturers Motorola has led developing M-Wallet Solutions. Its application allows users to download directly to their phones through their mobile Internet connections. M-Wallet includes such features as bill payment (linked to online bill-payment service providers), point-of sale payment, and money transfers, and would be funded by credit, debit, or gift cards stored in the phone. According to media reports, the solution also permits users to make payments from prepaid wireless accounts, or have payments charged to their monthly phone bills. Motorola must now broker deals with wireless carriers and issuers to bring the service to end users. Motorola is currently running a pilot with Morgan Stanley that will allow 1,000 Discover Card clients in the Chicago and Salt Lake City areas to use their Motorola phones as a means of payment.

However, where “transformational models” are being developed is when mobile virtual network operators (MVNOs) partner with prepaid providers. As resellers of wireless services, MVNOs frequently target niche markets such as youth and ethnic minorities that mobile operators would otherwise have difficulty accessing. Consequently, MVNOs may prove particularly suited for banking the unbanked among their customer bases. They may also provide major mobile operators with the opportunity to experiment indirectly with mobile banking without the risk of public failure.

AMP’d Mobile, a youth-oriented MVNO with a focus on multimedia content, has announced a partnership with mobile payments company Obopay. Virgin Mobile, another youth-focused carrier, will launch a prepaid Visa debit “Stash” card with prepaid provider NetSpend. The product’s mobile-based features include P2P transfers and text-based account alerts. Movida, an MVNO targeted to the Hispanic market, has plans to offer a mobile-linked prepaid debit card that will facilitate top-ups and provide an opportunity to develop credit for the unbanked population. Movida’s m-payments solution will also integrate the prepaid debit card and phone to provide wireless remittance services, in addition to wireless transaction and balance alerts.

Finally, in the past two years, a number of mobile-oriented financial services companies have entered the market or announced their intention to do so. Most are start-ups, some of which have received substantial venture funding. A notable exception is PayPal, which has leveraged its successful online payment platform with more than 100 million users to begin to provide mobile payments services (launched in April 2006). Paypal uses SMS or IVR technology in order to offer P2P transfers and merchant payments at participating retailers using their Pay Pal accounts. Currently the SMS service works on Alltel, Sprint, T-Mobile, and
Verizon. Text message payments might be attractive to offline merchants too small to afford credit card merchant accounts, and to online merchants having signed for Paypal merchant services.

Paypal Mobile leverages on the API platform developed by Paypal Merchant Services, the unit of Paypal in charge of developing business outside of the eBay payments world. Paypal was founded in 1998 and launched originally as a “person to person” electronic payments network. However, it soon became clear that Paypal’s most important revenue generating activity was servicing “online auction marketplaces.” It was attractive to auction sellers, most of which were individuals or small businesses that were unable to accept credit card payments directly from consumers. Many sellers could not qualify for a credit card “merchant account” because they lacked a commercial credit history; for others, the fixed fees associated with a merchant account would be onerous, given their small scale. PayPal offered auction sellers a quicker and more convenient payment method. With PayPal, sellers did not need to wait to receive checks or money orders by surface mail before shipping goods. The service also appealed to auction buyers because they could fund PayPal accounts using credit cards or bank account balances, without divulging credit card numbers to unknown sellers. Sharing personal financial information was a serious concern that led many consumers to avoid buying online.

In July 2002, online auction leader eBay—conceding the defeat of its Billpoint service created to compete with Paypal—acquired PayPal for $1.4 billion in stock and shut down Billpoint. PayPal's first-mover advantage and torrid viral growth caused not only Billpoint but also many other early online payment rivals to fall by the wayside. As a result, paying in eBay became the “killer” application that Paypal needed in order to achieve enough scale and become a serious competitor in the “off-e-Bay” world.

At a February 2005 analyst conference, PayPal management described the off-eBay opportunity, citing Forrester research that estimated 2004 U.S. e-commerce spending to be $144 billion, with eBay garnering a 12% share.26 The research further segmented the U.S. off-eBay market into three groups based on annual online sales: sole proprietors (less than $250,000), small-to-medium businesses ($250,000 to $5 million), and large merchants (more than $5 million). Merchant services would target small-to-medium and large online merchants, which together made up $116 billion in off-eBay U.S. sales. In these markets, credit cards were the dominant payment solution.

The Pay Pal Merchant services strategy was based on the development of the Website Payments Pro Merchant Services launched in June 2005. Pay Pal Merchant services were targeted at small and midsize

---

26 Harvard Business Review, 2006
online merchants that demanded more control over their transactions. The Pro product suite featured two new functions: Express Checkout and Direct Payment API. Express Checkout allowed shoppers with PayPal accounts to pay for items and supply shipping information with just three clicks at merchants’ websites. Direct Payment API let sellers accept credit cards from buyers who did not have PayPal accounts, then process those payments through the PayPal system and deposit them into merchants’ PayPal accounts. With Direct Payment API, PayPal offered a one-stop alternative to traditional credit card acquirers, merchant processors, and gateways.

Recent investments in the online world are solidifying PayPal Merchant services strategy as an “off e-Bay” payment system. In October 2005, PayPal announced its acquisition of VeriSign’s payment gateway business for $370 million, boosting its transaction volume and acquiring a large base of online merchants to which Merchant Services could cross-sell its products, including Website Payments Pro. In July 2005, eBay purchased a leading U.S. comparison-shopping site, Shopping.com, for $620 million. In September 2005, eBay acquired Skype, the world’s leading voice-over-Internet-protocol (VoIP) provider, for $2.6 billion.

Mobile banking technologies

In the U.S., Near Field Communications (NFC) technology, consisting of “standards-based short-range wireless connectivity technology” that permits communication between enabled devices is driving the development of the industry. Mobile banking technologies in developing countries such as the Philippines, where the industry has developed extensively, are based on SMS technology. In Japan, the developed country with the highest penetration of mobile banking, the industry has developed also using NFC technology. For its use in mobile phones, NFC chips may be attached to headset covers or incorporated directly into phone hardware.

Currently, NFC technology is already being used in tags, fobs, and cards such as Mastercard’s successful PayPass product, but it also enables additional mobile functionality. As a result, the merchant locations that currently accept contactless payments (including a number of high-profile fast-food and retail chains) will in theory be able to receive payments from NFC-enabled phones. Like existing contactless payments products, NFC will likely leverage the card-payment networks already in place by linking to users’ association-branded cards.
A significant development for the use of Mastercard’s successful PayPass product in mobile banking comes from Giesecke & Devrient42 (G&D) and MasterCard International,27 which announced the development of a secure over-the-air (OTA) personalization scheme. PayPass can be enabled directly with the customer’s phone, making a one-time request to their bank to register for the service. Data is sent over the carrier network and then automatically loaded and activated by PayPass payment application in the mobile phone while personalizing the phone’s built-in “secure area” with the customers’ card payment account details. This technology permits card issuers to securely load accounts to customer’s mobile phones without accessing the phone’s SIM card or creating vulnerabilities for the phone’s NFC chip. During the first quarter of 2007, Citibank, MasterCard, and Cingular began testing the technology in the New York City market using NFC-enabled Nokia headsets.

Unlike the contactless payment cards currently available, phones with built into NFC devices can be linked to “mobile wallets” that allow access to multiple accounts or cards. Limited by definition to local (non-remote) transactions, NFC technology can be also be used to “top up” prepaid mobile accounts at merchant load stations, or to facilitate in-person transfers between two users with NFC-enabled headsets. Supporters of NFC maintain that the technology will prove more user-friendly than SMS-based payments at point of sale and be processed even faster than traditional cards or cash. Broader adoption, however, will require certification of the technology, standardization across mobile carriers and financial institutions, and, most notably, substantial investments by retailers in POS infrastructure.

An alternative to SMS and NFC technology is to provide access to online banking and payment platforms through users’ mobile phone internet browsers. However, this solution is creating little enthusiasm in the industry since online content must be resized to fit small-screen cell phones, most likely through the creation of dedicated websites. Besides, the relatively slow speed of many users’ mobile-based web access may also be a significant obstacle. The final barrier is cost, since mobile users connecting to the internet generally pay substantial fees.

**Conclusions: Mobile Banking and the Underbanked-Partnerships Between Prepaid Card Issuers and Mobile Operators Will Shape the Future of Mobile Banking in the U.S.**

Mobile banking has a potential market segment in the U.S., already targeted by prepaid issuers. The customers that are not being currently served by the traditional banking sector could be interested in this

---

27 Mastercard International and Global System for Mobile communications Association have launched a global initiative to let international migrants transfer money home through their cell phones
value proposition if it fit their demands. Among the unbanked, Hispanics are potentially the segment of the population that mobile banking emergent initiatives are currently targeting. Banking access and mobile phone usage of Hispanics in the U.S. is very similar to banking access and mobile phone usage in some developing countries such as South Africa, where mobile banking has made important inroads.

As many as 40 million American households are underbanked. At the same time, a 2004 Mintel report shows that 65% of Americans own mobile phones. Because of the strong relationship that still exists between mobile phone ownership and income, it does not automatically follow that 65% of the underbanked are mobile phone users. A more cautious estimate rests on Mintel’s finding that 44% of Americans with a household income of under $25,000 have cell phones. Assuming, quite conservatively, that only 40% of underbanked households include at least one mobile phone user, the existing market for underbanked mobile banking would exceed 17.5 million people.

Hispanics over the age of 18 without bank accounts that have mobile phones are approximately 3.7 million consumers. This estimated purely “unbanked” population excludes the millions of Hispanics that have some kind of banking relationship but continue to use alternative financial services, such as check cashers and money-transfer operators. They too, could derive significant value from mobile banking offerings targeted to the underbanked. As a result, Hispanics likely constitute at least one-third of the potential mobile banking underbanked market.

Though no definitive data exists on cell phone usage among the underbanked, mobile technology has become increasingly popular among the demographic groups most likely to be financially underserved by the traditional banking system. The market research firm Mintel shows that in 2004, 57% of Hispanics owned mobile phones. Further, according to the Pew Internet and American Life Project, young and non-white users are significantly more likely than young and white users to claim that “they can’t live without their cell phones.” The Pew study also identifies a subpopulation of “cell only” users who do not have land lines (largely for financial reasons) and who are “disproportionately male, under age 30, non-white, unmarried and from households . . . earning less than $30,000.” A study by the Tomás Rivera Policy Institute notes that of all ethnic groups in the United States, Hispanics are the most likely to give up land

31 Mintel Reports, “Mobile Phones.”
lines in favor of exclusive mobile phone use. They also tend to have the highest average wireless bills, at approximately $71 per month, an indication of the intensity of their mobile use.

“Cell-only” users tend to use their mobile phones for a greater range of services, including text messaging and internet applications—two key platforms for mobile banking. Indeed, 61% of cell-only users employ text-messaging, compared to 31% of cell users with land lines; cell-only users are also far more likely to use their mobile phones to access websites and send e-mail. Minority groups and younger users appear to share these preferences.

Partnerships between prepaid card issuers and mobile operators will shape the future of mobile banking in the U.S. In many ways, preloaded mobile payments solutions closely resemble prepaid cards. Indeed, they may provide similar benefits to users: better security than cash, reduced risk of overdraft or penalty fees, convenient loading of value, and, in the case of the most advanced cards, opportunities to save, transfer funds among users, and build credit history. Indeed, the line between prepaid cards and m-payments could prove hazy, as many prepaid companies begin to contact customers through text messaging, while at the same time many m-payments platforms, such as Obopay, seek to overcome the hurdle of POS accessibility through the issuance of branded prepaid cards.

One of the most natural applications of mobile banking technology, then, may be to build on existing prepaid infrastructure, leveraging mobile technology to provide greater accessibility and functionality to prepaid products currently marketed to the underbanked. These partnerships would allow mobile banking value propositions to take advantage of the experience of issuers of prepaid cards in the Hispanic market, designing products specifically tailored for this segment of the population. In addition, alliances between issuers of prepaid cards and specialized mobile virtual network operators would allow both to benefit from income and operational synergies. Besides, by partnering with issuers of prepaid cards, mobile banking value propositions would be able to include services such as merchant pay, bill pay, remittances, person-to-person (P2P), prepaid top-up and tie-ins, short term credit, and even savings.

The most important challenge that would need to be overcome in order to create competitive value propositions based on the mobile banking business model identified is to build extensive load networks. For underbanked users of mobile financial services, the ability to easily load money to their phones may prove as important as the ability to spend and transfer funds. Customers without bank accounts or credit

33 Mintel Reports, “Mobile Phones.”
cards—the most common source of funds for existing mobile banking platforms—will require alternative load mechanisms.

Prepaid load networks such as check-cashing outlets, direct payroll deposit, designated kiosks, or “reverse ATMs” that accept cash and point-of-sale loads through partnerships with retailers could be leveraged in order to build extensive load networks. Some mobile banking providers have already started thinking along these lines. Though the service is not currently offered, Obopay envisions a strategic partnership with a payroll card company that would enable customers to receive their salaries directly deposited to their mobile accounts. Retailers like convenience stores and discount chains, already beginning to offer transactional financial services, could provide a particularly valuable link to mobile banking services for this segment, not only as recipients of payments but also as load and unload locations. Because the underbanked already use these kinds of retailers extensively, they represent a promising point of customer service for mobile banking.