American Bankers Association®

The Changing Face of the Payments System:

A Policymaker's Guide to Important Issues

About the ABA and this Paper

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

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

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

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

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

The Evolving Payments Market

Background

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

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

Innovation

Our once cash-based society has evolved through checks, into cards, and is now pushing into a digital frontier of virtual "wallets"[1] and mobile platforms. Innovators span the gamut from traditional players doing new things to new players performing similarly traditional functions (e.g., PayPal, Square), while at the extreme end, others are attempting to bypass the existing payments system entirely (e.g., Bitcoin). The common thread is that all of them are continually seeking new ways to assist consumers and businesses in the way they make purchases. Banks—which developed the first credit card in 1958 and have since pioneered technologies like online banking and billpay, mobile banking, and remote check deposit capabilities—continue to push the innovation envelope to improve the banking experience for consumers and businesses. Additionally, several large nonbanks are now active in the payments sector, including PayPal, Walmart, Google, Square, and telecommunications operators such as AT&T, Verizon and T-Mobile. With so much activity, the most successful will be companies that deliver superior benefits to the overall payments ecosystem.

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

Implications

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

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

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

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

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

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

1. Consumer Protection

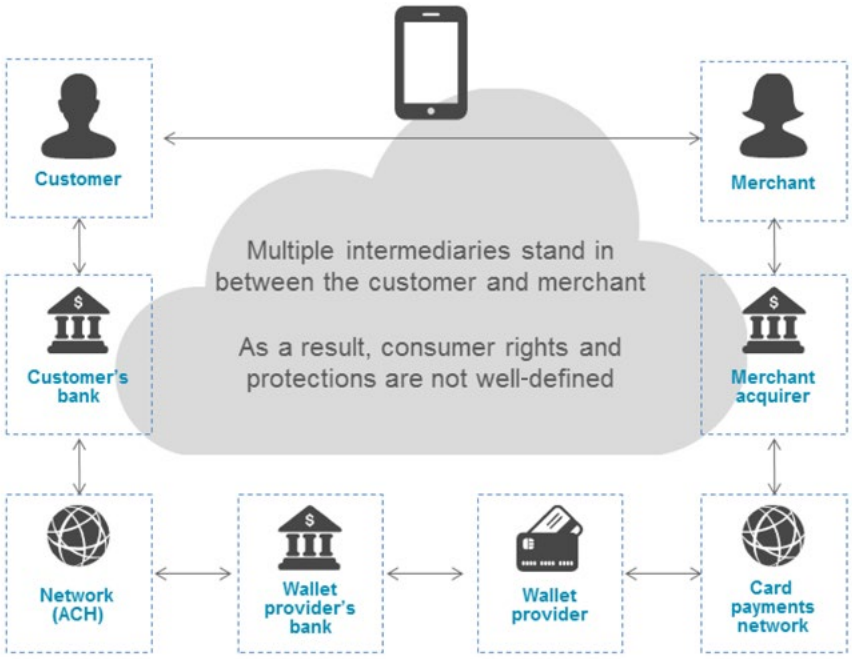
Key Questions:

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

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

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

Mobile wallet transaction involving a pre-funded wallet



Existing Protections Establish Clear Consumer Rights

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

Newer Technologies, Unclear Rules

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

For example, a nonbank payment provider may link a smart phone service to a conventional bank service, such as ACH, debit transactions or a credit card or debit card. These may be two separate transactions. The nonbank payment service provider pays the merchant and, in a separate payment transaction, the customer's bank pays the nonbank payment service provider. Nevertheless, these two transactions may be perceived by the consumer as a single transaction. However, the nonbank transaction may not be subject to the consumer protections of the Electronic Funds Transfer Act (EFTA).[2] Even if the EFTA applies, or the nonbank payment service provider treats it as applying, consumers are almost certain to be confused about how to assert their rights for errors or unauthorized transactions. For example, if an unauthorized or erroneous transaction occurs, should consumers go to their bank or the nonbank service provider? Will their bank, which paid the nonbank service provider, be able to identify the merchant that was paid by the nonbank payment service provider (as sometimes this information is hidden from the bank), or have a process for resolving the dispute with that merchant?

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

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

2. Payment System Integrity

Key Questions:

- **Does the nonbank payment provider adhere to all government and regulatory programs to maintain the safety and soundness of the payment system?**
- **If not, and because the provider currently falls outside the existing payments regulatory framework, does the provider introduce a potential weak link into efforts to safeguard the U.S.?**

Marketplace Evolution

To borrow from the old saying: a payments infrastructure is only as secure as its weakest link. As online payments and mobile payments become more popular, consumers are increasingly storing their payment credentials[3] on multiple websites. And as the vulnerabilities of payment card magnetic stripes continue to be exploited in larger numbers, issuers are looking to technology to improve their fraud protection capabilities.

Here are some examples of developments in the marketplace:

- To pay online, consumers create an account with the e-commerce provider and register their payment card(s). Now, when it's time to pay, consumers can simply check out rather than having to enter their card information, billing address, shipping address, and other relevant details. In this way, Amazon, Apple's iTunes and other online retailers reduce "friction" in the consumer shopping experience.
- Brick-and-mortar retailers are also encouraging customers to register their payment cards, either to receive discounts or to link them to the merchants' loyalty programs.
- Increasingly, mobile wallet providers require consumers to store their account details on their smart phone (or make them accessible to the phone), so that the phone can be used to initiate payments.
- Payment card networks, card issuers and merchants in the U.S., seeking to keep pace with evolving technologies and increasingly savvy criminals, are—among other things—in the process of implementing a chip technology known as EMV (see the sidebar on the next page).

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

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

Fighting Card Fraud in the U.S.: Evolution to EMV and Beyond

After years of talk, there is now a renewed push to migrate the U.S. payments market away from magnetic-stripe payment cards and toward chip-based payment cards. The global standard is called EMV, short for Europay, MasterCard, Visa.

- As chip cards are much more difficult to counterfeit than traditional payment cards, both banks and retailers may enjoy lower fraud losses by utilizing this technology.
- EMV is already a global standard, with more than 1.5 billion chip-enabled cards issued.
- However, EMV does not prevent or deter fraudulent card-not-present purchases, such as online shopping.
- Payments fraud is an evolving challenge, with criminal networks constantly seeking new ways to exploit perceived "weak links" in the system. For example, evolution to EMV is but one proposed step in the fight against fraud and has been around for nearly two decades. As criminals adapt to changing protection schemes, new counter-measures must, and are, being developed.
- The key is to develop the best market-based solution(s), and to ensure that all payment system participants embrace the challenge.

System Security

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

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

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

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

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

Identifying the Merchant

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

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

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

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

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

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

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

3. Competitive Equity

Key Question:

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

Regulatory Differences

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

- Depository institutions have an extensive system of regulation and supervision of their controls and ability to carry out payments system services, designed specifically to protect the industry's safety and soundness.
- They are likewise subject to a stringent consumer protection regime that ensures adequate disclosures, limits fraud liability and protects a customer's privacy.

On the other hand:

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

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

Barriers to Enhanced Competition

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

One illustration of this is the so-called Durbin Amendment, which imposed price controls on debit card interchange revenue for only certain market participants (i.e., banks with over $10 billion in assets) and certain products (i.e., debit cards). This creates market incentives to innovate away from certain products (i.e., debit cards) and towards other products (i.e.,

prepaid cards). It likewise forces some market participants to limit the consumer utility of their products—in this case, for example, some larger banks cannot offer prepaid cards with automatic bill-paying functions without being subject to Durbin price controls, while others face no similar revenue restriction. In the end, it's consumers that lose as they no longer have the option to choose beneficial products from the widest range of competitors. Such arbitrary line-drawing by policymakers restricts the ability of all market participants to compete on equal footing, denying consumers the benefit of that innovation and competition.

The Big Picture

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

Conclusion

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

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

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

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

1120 Connecticut Avenue, NW | Washington, DC 20036 | aba.com | 1-800-BANKERS