



Research Brief

MOBILE REMOTE COMMERCE:
ADDRESSING THE CHALLENGES

THE PAYFONE SOLUTION

Glenbrook Partners
December 2012

Table of Contents

Abstract	3
Mobile Commerce	4
Mobile Payments Landscape	4
<i>Mobile Remote Commerce</i>	5
eCommerce – the Precursor Market	7
<i>Card-Not-Present Transactions</i>	7
<i>eCommerce Fraud Risk Management</i>	8
<i>eCommerce Fraud Management Tools Used</i>	9
<i>From eCommerce to Mobile Remote Commerce</i>	10
Mobile Remote Commerce - A Market Emerges	10
<i>Mobile Remote Commerce – Consumer Segments</i>	11
<i>Mobile Remote Commerce – Merchant Segments</i>	12
<i>Online-Offline Convergence</i>	13
<i>Mobile Remote Commerce – Growth Drivers</i>	14
Mobile Remote Commerce Challenges	15
<i>Consumer Challenges</i>	15
<i>Merchant Challenges</i>	16
Payfone Solutions for Mobile Remote Commerce	18
About Glenbrook	20
<i>About the Authors</i>	21

Abstract

Mobile remote commerce is beginning to emerge as an increasingly important new retail channel, with the potential to generate significant sales for sellers and payment volume for financial services players.

However, this new channel presents certain unique challenges for payment systems, particularly with the respect to the potential for fraudulent use of payment cards and other financial accounts.

Payfone has developed a number of customized solutions which utilize unique data elements available from the mobile data network to more accurately assess whether a given payment transaction is legitimate, and can do so in a way that is highly convenient for the buyer.

Mobile Commerce

Mobile phones are having a dramatic, and much reported-on, impact on many aspects of commercial behavior, including both shopping and payments. Not surprisingly, there is considerable confusion about the various solutions emerging in the market.

Mobile Payments Landscape

Mobile remote commerce should be distinguished from other types of mobile payments. These include:

■ Mobile Payments at the Point of Sale

The consumer uses a mobile phone as a means of paying a merchant at the point of sale. Typically, the phone is associated in some way with one or more cards or other existing payment methods used by the consumer. This is sometimes referred to as *proximity payments*. There are two significant versions of this approach:

- **NFC Secure Element Payments** – a consumer's card or other payment data has been provisioned onto a secured chip on the phone, and is accessed by a wallet application. The card data is conveyed to the merchant terminal using NFC (Near Field Communications) technology. This method is considered to represent a *card-present* transaction by the card networks.
- **Cloud Based Payments** – a consumer's card or other payment data is stored in the cloud (by either a payments services provider or by the merchant) and the phone provides the merchant some form of token or link to the remotely stored data. (In another variant of this, the data is stored on the phone itself in an encrypted file, but not on the "secure element" referred to above.) When used with a card from a branded, multi-merchant network (such as Visa), these transactions are deemed *card-not-present* transactions by the card networks. The significance of this distinction is discussed below. Cloud wallets can also be used to hold merchant-specific payment instruments, which can be thought of as "mobile gift cards".

■ Mobile P2P Payments

The consumer uses a mobile phone to send a payment to another person. There are many mobile P2P solutions providers, including retail banks, online wallet services, and stand-alone P2P products. Although there are many variations on how the payment is initiated, the sender will typically use the receiver's phone number as an identifier. The receiver will receive a text message informing him that he has received a payment; if he is not yet an account holder with the provider, he will be asked to set up an account to receive funds. The sender may be given the option to fund the transaction by a bank account or a card. Significantly, mobile P2P payment solutions are being promoted by providers as a means to pay personal vendors or micro-businesses, in competition with the "mobile payments acceptance" solutions described below.

■ Mobile Payments Acceptance

The receiver of funds uses a mobile phone as a means of accepting cards at the point of sale (or POS). The phone is equipped with a device to read a magnetic stripe swipe (or, in EMV countries, to accept an EMV chip card). The transaction may be deposited into a specialized form of merchant account from the solution provider, or may be linked to an existing merchant account. These transactions, when used with an acceptable device to read the magnetic stripe or chip, are considered *card-present* transactions by the card networks.

Mobile Remote Commerce

Mobile remote commerce is one of the important sectors of this developing market. In mobile remote commerce, a consumer is using a mobile device to make a purchase, remote from the merchant and the merchant's physical point of sale acceptance environment. The consumer may be using a phone browser or an app on the phone; the app may be provided either by the merchant or a third party. This definition of mobile remote commerce spans mobile devices and tablets connected via 3G, 4G, or Wi-Fi.

The consumer may pay for the purchase in a number of ways:

- By using an online wallet service
- By using a “card on file” with the merchant
- By directly entering card payment information
- By using a private label/gift card issued by or on behalf of a specific merchant

Mobile remote commerce may even occur when the consumer is physically present at a merchant: consider, for example, a consumer using a phone to make a remote purchase while in the aisle of a “big box” store.

It is important to note that the first three options create what the card networks consider to be *card-not-present* transactions: the significance of this will be discussed in the following section.

eCommerce – the Precursor Market

Mobile remote commerce can best be understood in context of the established eCommerce, or online shopping, market. When the eCommerce market began to develop, in the mid-1990s, it was itself an outgrowth of the existing mail-order and telephone-order marketplace (once referred to as the “MOTO” channel). It was within this MOTO channel that the card networks developed the concept of *card-not-present transactions*: this concept carried forward to apply to eCommerce, mobile remote commerce, and cloud-based mobile point of sale transactions.

Card-Not-Present Transactions

Card network rules have special provisions for *card-not-present* transactions. The distinction, technically, is not the physical presence of the card, but whether or not the merchant terminal has “read” the magnetic stripe (or chip) holding the card account data in a manner acceptable to, and certified by, the card network. Where this has not occurred, the transaction is considered a *card-not-present* transaction.

The merchant takes fraud liability on “card-not-present” transactions even when it is the consumer who is acting fraudulently – such as when a consumer actually did a transaction, but later claims that they did not.

The most important of the special rules on card-not-present transactions is the allocation of liability for fraud, in particular, unauthorized use of the card. A cardholder complaining to his card issuer that “I didn’t do it” has his account credited, and the transaction is *charged back* by the card issuer to the card acquirer, which then debits the merchant’s account. (The same cardholder complaint, in a card-present transaction, is handled by the card issuer: if the issuer credits the consumer’s account, then the issuer takes the loss.)

Because of this risk exposure, an eCommerce merchant must carefully scrutinize transactions (even those initially approved by the card issuer) and decline sales if fraud is suspected. The merchant faces a dilemma: an aggressive fraud management posture (declining many sales) risks turning away good business and insulting good customers; a lenient approach risks significant losses from sales for which payment is never received. As the eCommerce market grew, an increasingly sophisticated set of practices and solutions evolved to help merchants make these decisions, and manage these risks.

eCommerce Fraud Risk Management

The solutions used by eCommerce merchants for fraud risk management vary by the size of the merchant and the type of goods being sold.

We classify eCommerce merchants into four segments, each of which has unique requirements for online payments acceptance, and for fraud management. The potential for cross-border revenue also varies from segment to segment.

- **eRetail** merchants use “shopping carts” and ship physical goods. They need to manage the complexities of this environment; with typically high costs-of-goods sold, these merchants are particularly vulnerable to fraud, although they do have the option of mitigating fraud through delay of shipment of goods
- **Travel & Entertainment** merchants have specialized websites to allow consumers to choose booking options. These merchants are also highly susceptible to fraud, particularly when a ticketed event occurs immediately after booking.
- **Online Services** merchants normally keep a payment card on file, which is charged monthly. There are many sub-segments here, but generally these merchants are less vulnerable to fraud, managing their exposure by simply turning off service as soon as fraud is detected.
- **Digital Content** merchants may sell music, video, games, magazines, etc. They are similar to online services merchants but sales are usually done “per bite.” These merchants typically have a relatively high gross margin and low cost-of-goods sold, making them less exposed to financial loss from fraud. It should be noted, however, that many digital content merchants do have some costs-of-goods sold from royalty or licensing obligations.

Not surprisingly, fraud management practices vary significantly by segment. There are vendors that specialize in solutions for each of these segments. In addition to varying fraud exposures by segment, fraud management practices vary by the size of the merchant. In general, very large merchants buy component solutions, and integrate them in-house into decision engines supporting online sales. Small merchants are more likely to buy packaged solutions from gateway providers, PSPs (payments services providers), or card acquirers.

Cross-border risk exposures are particularly challenging. Many merchants simply decline cross-border business, or accept sales from only a narrow set of countries. Global PSPs have emerged to help merchants access local country

payment methods, and to manage the particular risks with each payment system.

eCommerce Fraud Management Tools Used

As eCommerce has matured, a robust set of fraud management tools has become available for online merchants. The use and efficacy of the tools evolves over time, as new technologies become available and, significantly, as fraudsters learn to work around new tools. The primary categories of these tools are as follows:

Fraud Detection Tools	Use or Planned Use of Tools	
	By All Merchants	By Large Merchants
Validation Services (CVN, address, etc.)	97%	100%
Proprietary Data/Customer History	67%	89%
Multi-Merchant Data/Purchase History	30%	51%
IP geolocation information	58%	88%
Device "fingerprinting"	41%	83%

Source: 2012 CyberSource Fraud Report

Device fingerprinting and IP geolocation were cited most often by large eCommerce merchants as their most effective tools for mitigating fraud.

- Device fingerprinting is a technique used to establish a “fingerprint” of a user’s computer or other web access device and involves collecting attributes such as IP address, browser settings, operating system, software version numbers and other unique, identifiable traits of the device
- IP geo-location uses the geographic location of the user from the IP address of the user engaged in the eCommerce transaction. Typically fraud management systems trigger an alert when activity is coming from an unauthorized country or through a proxy.

From eCommerce to Mobile Remote Commerce

Mobile remote commerce, in some instances, is simply an extension of eCommerce: a consumer using a mobile device, rather than a desktop or laptop computer, to remotely purchase goods or services.

But as we will see, mobile remote commerce will also include new types of commerce: new groups of consumers, new types of merchants, new types of risks, and new solutions for risk management.

Mobile Remote Commerce - A Market Emerges

Mobile remote commerce is clearly in its early stages, but there are promising signs of growth, and impressive potential, particularly in the developed markets. Smartphones, and shopping apps in particular, are an important development.

Many merchants have gone through an evolution in supporting remote mobile commerce:

- Browser on phone – manual data entry by consumer
- Web optimized browser – simplified choices for consumer, tailored to mobile form factor
- Simple shopping app – allows consumer to browse through merchandise
- Advanced shopping app – supports embedded payments options and/or online wallet checkout

Each stage in the progression simplifies the consumer's choices and makes selecting goods and purchasing easier. Because of this, we should be cautious about projecting market volumes and growth rates from earlier stages onto later stages.

Total mCommerce sales for 2012 are estimated to be \$21 billion.

Source: Internet Retailer Mobile Commerce Top 400, September 26, 2012

Mobile Remote Commerce – Consumer Segments

So which consumers will use their mobile device to shop? We see at least three notable segments:

- **The All-Digitals** – consumers who are avid users of both computers and mobile devices. They are likely to own both smartphones and tablets. They will demand the ability to move smoothly between devices, using the same authentication and payment methods. They will expect, for example, unified offers and coupons when shopping at a merchant’s online and mobile stores.
- **The Mobile-Preferred** – consumers who use both computers and phones, but prefer to use phones. This is the group that wonders, “Where are the apps for my computer?” They will be less sensitive to the need to have common experiences across computer and phone. Logically, many younger people will fall into this segment.
- **The Mobile-Only** – consumers who do not use computers on a regular basis. This includes “non-desk bound” adults, some lower-income families, and some young people. Interestingly, statistics are emerging showing that tablets are replacing computers for many people.

Certain **types** of goods and services also have a higher propensity for mobile commerce:

- Time sensitive services (e.g., flash sales)
- Mobile delivered goods (e.g., tickets)
- “Mobile Native” apps – that do not exist on the online channel (e.g., geolocation apps)

Who will **not** be using their phone to shop? Many people who today do not shop online for reasons of security (as opposed to those without easy access to computers) will probably not shop with their phone. Furthermore, a segment of those who do shop online may feel that mobile commerce is more risky: this may change with time, mirroring the progress of eCommerce, where many early, fearful skeptics became online buyers. Finally, there is a segment of people, many older, who made the transition to the use of computers but find mobile devices overwhelmingly complicated – and small!

Mobile Remote Commerce – Merchant Segments

How should we think about the merchants that will sell to these consumers? Although it seems obvious that any eCommerce merchant will want to also support mobile remote commerce, there are some variations that are important to consider.

- **eRetail** merchants, in addition to having mobile shopping sites and apps, will also want to deliver coupons and offers to consumers. These marketing programs may be integrated across channels or be mobile-specific (such as in the case of proximity offers), and they may be payments-integrated (such as with Google Wallet or Isis Wallet) or payments-independent (such as Groupon).
- **Travel & Entertainment** merchants can expect to have many mobile remote shoppers. Already, travel booking sites are reporting high levels of bookings coming from mobile devices. Specialized event apps (e.g., stadium ordering) will be common and mobile-only. Significantly, large segments of restaurants, particularly fast-food and take-out restaurants, will have proprietary ordering apps allowing consumers to order remotely for in-person pickup later (e.g., OLO).
- **Online Services** merchants will need to support mobile service delivery for access to premium features, as well as new customers signing up from mobile devices.
- **Digital Content** merchants can expect very high use of mobile devices from both existing and new customers.
- **Traditional store-based retailers** are increasingly using the remote mobile channel to redefine the competition versus traditional online only retailers.

In addition to merchants currently supporting eCommerce, we can expect to see some merchants supporting only mobile remote commerce

- **Physical delivery** merchants, who rely on immediate physical delivery of goods, may have never thought a website made sense, but will use mobile apps (especially those integrated with couponing or mobile offers), to support their current business: coffee shops, delis, clothing and household goods boutiques, etc.
- **Digital content** merchants that realize most of their revenue from the sale of apps to consumers, and are expanding into in-app purchases, may migrate some of their business off those platforms and onto direct mobile remote commerce channels.

Online-Offline Convergence

Merchants and consumers alike will be drawn into scenarios where the use of the mobile device makes “online-offline convergence” not only possible, but easy. In fact, it is clear that mobile devices are a driving factor in the blurring of the lines between traditional retail, eCommerce and mobile commerce. Some of these scenarios are happening now, some are just emerging, and some are “around the corner”.

- Consumers who use their mobile phones to scan items in stores, and then buy later, online.
- Consumers who shop online, and then go to stores to purchase; sometimes, the purchase is done online and only the pickup is local.
- Consumers who buy with mobile devices “in the aisles” from the remote mobile app or site of the retailer.
- Consumers who buy, via mobile remote commerce, from competitors of the retailer (a practice increasingly known as “showrooming”).

One of the more significant components of the “Online to Offline” convergence discussion are the mobile “Cloud Based Payments” solutions being used at the point of sale (discussed above on page 4). Although these solutions are not thought of as “remote”, the fact that the card networks classify the purchases effected with them as “card-not-present” transactions means that the merchants are faced with the same risk management profile that exists with mobile remote commerce or eCommerce.

Mobile Remote Commerce – Growth Drivers

What will drive the growth of mobile remote commerce? In addition to the obvious mobile-centricity of the consumer, there are a number of other factors that we believe will have a significant impact:

- The ongoing popularity of eCommerce and online services, and a related comfort level with the safety of online shopping, will make the mobile adoption curve less steep.
- The proliferation of connected mobile devices (including both smartphones and tablets) will drive a virtuous circle of application development and use.
- The increasing speed of mobile data networks and the prevalence of public Wi-Fi networks will enable “anywhere” mobile remote commerce.
- The use of voice commands will offset some of the difficulties of navigating small screens.
- Ongoing investments by traditional retailers in mobile enhancements to the in-store shopping experience.

Mobile Remote Commerce Challenges

Mobile remote commerce does, however, present certain unique challenges for consumers, merchants, and payments providers.

Consumer Challenges

The small size of the mobile device can make consumer data entry difficult:

- A new customer, or an existing one electing to use a “guest checkout”, will face a daunting data entry challenge in order to make a purchase. First, customers will need to establish log-in credentials acceptable to the site. Then, they will need to manually enter checkout information – card number, expiration date, card validation number, bill-to address, ship-to address, phone number, etc.
- A returning customer using a mobile website or app will still face a significant amount of data entry on a mobile device in order to complete the typical “username and password” login.
- Contact and shipping information will typically be held on file, but payment card data may still be required, unless the customer has seen fit to put that information on file with the merchant.

The failure to provide a streamlined checkout experience tailored to the mobile form factor is already resulting in high abandonment rates, rates far higher than those experienced by eCommerce merchants.

Merchant Challenges

Merchants engaging in mobile remote commerce face the risk of fraud.

Intuitively, given the newness of the channel, mobile fraud is probably quite high. Disturbingly, however, 92% of merchants do not know their mobile fraud rates.¹

High mobile fraud rates reflect both the predictable movement of fraudsters to the new channel, but also the relaxed attitude consumers have to security on their mobile devices.

Over 50% of mobile phone users keep passwords, credit card details, and personal information on their phones. Moreover, the risk presented by lost or stolen phones (over 70 million each year) is particularly high: lost and stolen phones contain sensitive data: 62% have contact lists, 58% emails, 52% have internet credentials,, 35% security codes and settings, 34% business apps, and 30% mobile payments related data. ¹

Merchants, particularly current eCommerce merchants, will naturally turn to the tools used to manage eCommerce fraud to manage the risks in this new channel. They will find, however, that there are new vulnerabilities in the mobile channel that cannot be fully addressed by the fraud detection tools used for eCommerce.

Fraud Detection Tools Used for eCommerce	Use or Planned Use of Tools		Applicability to Mobile Remote Commerce
	By All Merchants	By Large Merchants	
Validation Services (CVN, address, etc.)	97%	100%	Yes, with limitations, and/or modifications required
Proprietary Data/Customer History	67%	89%	
Multi-Merchant Data/Purchase History	30%	51%	Yes
IP geolocation information	58%	88%	No
Device "fingerprinting"	41%	83%	No

Source: 2012 CyberSource Fraud Report, Glenbrook Analysis

In the mobile channel, the use of some increasingly important fraud detection tools are either not relevant or are of limited value, even if mobile-specific, analogous tools are created.

¹ Source: CyberSource 2012 On-Line Fraud Report

- The ***mobile phone number*** itself is unreliable as a customer identifier, particularly when it is provided by the device. Ten percent of U.S. mobile subscribers change their mobile numbers every year, and wireless carriers recycle numbers to new customers. At the same time, devices can be hacked, cloned and otherwise made to present a false number.
- ***Device recognition*** can also be problematic. SIM cards are portable to different handsets; phones get lost and replaced; devices can be hacked and cloned.

The standard solution approach to similar problems in eCommerce is to add a secondary authentication process, such as requiring responses to challenge questions. This, of course, requires additional data entry by the consumer, which is again problematic on a mobile device.

So how can a mobile remote commerce merchant protect themselves from losses due to fraud?

Payfone Solutions for Mobile Remote Commerce

Payfone is a mobile commerce company that addresses the checkout process on mobile devices by linking mobile identity with the payment process to provide merchants and consumers with an easy, fast, and secure mobile checkout experience.

Payfone provides merchants with a mobile shopping solution that avoids interfering with their existing checkout process or sacrificing security in the payment flow. The company believes that proper multifactor authentication in the mobile domain should be capable of cross-examining three kinds of attributes:

- Something you know (password, CVV code, challenge questions, etc.)
- Something you have (the SIM card in your mobile phone, credit card in hand)
- Somewhere you are (geolocation)

Payfone's solution can authenticate the SIM (something you have) and the location (somewhere you are) by obtaining that information from the mobile network rather than the device.

Payfone's technology, known as "1 Touch Checkout™", takes a unique approach to mobile transaction authentication by tying the shopper's identity to both the mobile phone number and the SIM card, in order to both simplify the checkout process and add an additional layer of security to mobile shopping. Payfone's solution uses the unique data elements available from the mobile carrier and bank networks to help merchants more accurately determine whether a payment transaction is legitimate and make the checkout process more convenient for the buyer.

The solution can be added into the existing authentication scheme used by a merchant, card issuer, or payments services provider, which will need to validate the "something you know" factor (likely a password or PIN). Payfone's solution is:

- **Merchant friendly:** Retailers deploy Payfone's solution within their existing account structure — no new payment mark is required.
- **Easy for consumers:** There is nothing for shoppers to download or install; after registering once through their mobile banking

app, billing and shipping information is automatically linked to the mobile identity so purchases can be made in a few quick steps.

■ **Secure:**

- Payfone authenticates the device using unique network assets (to ensure that it is not spoofed or cloned) rather than prior downloads, browser headers, or hardware attributes.
- Payfone also determines the location of the device using network connectivity rather than device-resident systems, which can be spoofed.

Consumer data entry requirements can be varied adaptively, based on the merchant's preferences and the perceived risk in a given transaction. Using "1-Touch Checkout" the customer is offered a streamlined checkout, again based on device and location validation, but is required to enter a password or PIN.

Payfone's solution is different from other risk management solutions for mobile remote commerce in the following ways:

- Does not require merchant acquirers or payment gateways to directly integrate to a third-party wallet or payment "button"
- Requires consumer registration, but is not another wallet
- Works for purchases made online, on the mobile web, and from within mobile apps
- Has coverage across all mobile data networks and Wi-Fi connections.

* * *

There is tremendous promise for growth in online payments conducted on mobile devices, initially for remote commerce purchases and increasingly over time to include in-store transactions. However, new payment channels inevitably become targets for fraudulent activity and must be carefully protected with solutions uniquely tailored to the technical characteristics of the channel. Payfone offers solutions of this type that leverage the high-quality authentication methods currently available for the mobile channel, and package them in a way will also produce a more streamlined and convenient buying experience for the consumer.

About Glenbrook

Founded in 2001, Glenbrook focuses exclusively on payments consulting. In addition to acting as consultants, each of Glenbrook's principals has long experience as a senior executive in the payments business, having dealt with both strategy formulation and the day-to-day realities of execution under the pressure of budgets and timelines. Glenbrook helps its clients to track a number of related markets to assess trends, surface opportunities, and identify threats, and then develop aggressive responses to these forces. The company is able to do this by bringing to bear a valuable combination of specialized skills in payments, decades of hands-on experience, and a network of high-level professional relationships.

Glenbrook works across the payments industry – with banks, merchants, billers, processors, networks, alternative payment providers, and a variety of investors – as well as across all payment methods (card, ACH, alternative, Check 21/imaging). We have deep expertise in each payment domain from ecommerce, POS, bill payment, P2P, B2B, to income.

Glenbrook is the publisher of [Payments News](#), the "blog of record" for payments professionals, more than 12,000 of whom read it each day. In 2009 Glenbrook launched a companion blog, [Payments Views](#) featuring commentary on topical issues in the payments space.



the

Glenbrook's Payments Boot Camp program offers intensive "deep dives" into the world of payments. The Boot Camp is offered several times a year for the public, or as a private on-site workshop. More than 6,500 industry executives have attended to date. We recently launched a series of payments education webinars on special topics and published a book, *Payments Systems in the U.S.* See www.PaymentsEssentials.com for more information course schedules, and book purchases.

Learn more at www.Glenbrook.com

About the Authors

Bryan Derman



Bryan has worked as a senior executive, security analyst, and strategy consultant during his 25-year career in financial services. He has developed new strategies and innovative business models for banking technologies ranging from ATMs and debit card acceptance

to bill payment and payroll check cashing.

Before joining Glenbrook, Bryan served as vice president of strategic development for Cyota, overseeing the company's relationships with strategic partners including payment processors and card associations.

Before Cyota, Bryan worked for First Data Corporation (FDC) as senior vice president for deposit access products at First Data Merchant Services.

Earlier in his career, Bryan worked at NatWest Bancorp in New York, Morgan Stanley, and McKinsey & Company.

Carol Coye Benson

Carol is a founding partner of Glenbrook. Carol offers clients over 25 years of experience in product, marketing, and strategy development with leading financial services providers in both wholesale and retail banking. Before founding Glenbrook Partners, Carol was a managing director of the Global Institutional Services division of Deutsche Bank, in charge of marketing, client online services, and Internet development.



At Visa International, she led a group conducting early work on the use of credit cards online, and a project that pioneered database marketing and related consumer-privacy issues. Carol also founded and managed Visa's European product-development office, where she led a series of electronic-commerce and chip-card projects designed to bring European banks online. Earlier in her career, Carol worked at Citibank and Bank of America.

Carol is the Partner in Charge of Glenbrook's [Payments Boot Camp](#) program. This unique program provides executive training for professionals in the payments industry. Glenbrook Payments Boot Camps are held throughout the year both as public events and as customized, private sessions for clients. She is co-author of the book "[Payments Systems in the U.S.](#)".

Writings by Bryan and Carol can be seen on [PaymentsViews.com](#)