

**INTERNATIONAL BAR ASSOCIATION
ANNUAL CONFERENCE IN SINGAPORE
OCTOBER 14 - 19, 2007**

INTERNATIONAL SALES, FRANCHISING AND PRODUCT LAW SECTION
PRODUCT LAW AND ADVERTISING COMMITTEE

SESSION: ALTERNATIVE METHODS OF PAYMENT
THURSDAY, OCTOBER 18, 2007

INTERNET AND MOBILE PAYMENTS IN THE UNITED STATES

Emma H.C. Lee, Esq.
Schnader Harrison Segal & Lewis LLP
140 Broadway - Suite 3100
New York, New York 10005, USA
(212) 973-8000; elee@schnader.com

There are many alternative forms of payment available in the US, including smart cards and stored value cards. However, this paper will focus on the most popular and successful alternative form of payment over the internet, PayPal, and on mobile phone payments, also known as m-commerce. M-commerce is not popular in the US, at least compared to Asia and Europe, but their use is growing and is expected to be as ubiquitous as in Asia or Europe within the next few years.

I. Overview

A. Current Payment Landscape

The US is unique among developed countries in that a majority of its payment transactions are conducted with paper forms of payment. The most popular form of payment in the US after cash is checks. Regulators and financial institutions have been unable to persuade Americans to stop writing out paper checks and mailing them, which is an extremely inefficient process for many reasons and not cost-effective. However, the use of checks has started to decline over the last few years and, while they are mostly being replaced by electronic payments, which include credit cards, debit cards and direct debit, alternative methods of payment are also taking its place.

B. Growth of E-commerce – Shortcomings with Traditional Methods

One reason checks have started to decline is because of the internet, which has spurred a change in many consumers' spending and payment habits. It is estimated that over 70% of Americans are online today and 15 million adults buy or sell products on the internet every day.¹ E-commerce sales are expected to generate over \$100 billion this year.² Credit cards are currently the most popular form of payment over the internet. However, three factors have

paved the way for new methods. First, consumers are concerned about security and transmitting sensitive financial details over the internet. Second, the introduction of online auction platforms like eBay has dramatically increased person to person (P2P) transactions and individuals cannot accept credit cards. Third, the high discount rates charged by credit card companies have galvanized merchants to seek cheaper alternatives. Discount rates are a percentage of a merchant's sale that are taken by bank card networks such as Visa and MasterCard to cover the transaction costs of a credit or debit card payment. They are typically about 2% and most of it is to pay an interchange fee charged by the bank issuing the card. For merchants that deal primarily in micropayments (sales worth less than a few dollars), discount rates often wipe out any profits.

C. Solutions - PayPal

Many alternative forms of payment over the internet have been introduced to address these concerns, especially during the dot-com boom, but most have failed. The most successful and enduring alternative method to date is PayPal. One reason for its success is its ability to address these concerns. PayPal (i) allows consumers to make purchases without providing credit details to a merchant, (ii) provides a means for individuals to pay each other and (iii) has lower discount rates than credit cards.

D. Potential in Payment Industry has also attracted M-commerce

The transaction fees earned by financial institution on credit and debit cards have also caused other industries to take notice but for different reasons. Almost two-thirds of the US \$13 trillion Gross Domestic Product is personal consumption expenditures, all which involve payment transactions.³ These transactions are dominated by traditional payment methods and earned Visa and MasterCard \$36 billion in fees last year.⁴ Mobile payment service providers (MPSPs) are hoping to cash in on this market by encouraging consumers to utilize mobile phones for payment. Even though there are approximately 245 million mobile phone subscribers in the US, which is over 75% of the population,⁵ m-commerce has yet to catch on in the US. US subscribers are already using mobile phones as cameras, mp3 players, organizers, calculators and clocks and to play video games. MPSPs are hoping that subscribers will just as easily migrate towards using cell phones as wallets.

II. **Technical Execution of Alternative Methods of Payment**

A. PayPal

PayPal offers different methods for transmitting money without revealing financial details to the recipient. PayPal started in 1998 and was acquired by eBay in 2002. After its acquisition by eBay, PayPal emerged as the dominant market player. It has had to endure numerous legal battles and regulatory disputes during its brief existence but is now the industry leader in online payments in the U.S. PayPal claims to have over 150 million registered accounts and, in the first quarter of 2007, its total payment volume exceeded \$11 billion.⁶

In order to use PayPal, a subscriber must have an email account and a credit card, debit card or bank account. The subscriber must first open an account with PayPal and then register the credit card, debit card or bank account which will be used to fund or receive payments. If an online merchant offers the PayPal service, a consumer can choose PayPal at checkout, similar to selecting the option to pay via Visa or MasterCard, and does not need to provide any credit information to the merchant. The funds will be transferred from the consumer's PayPal account or from the designated credit card, debit card or bank account. Only the merchant pays transaction fees to PayPal. This is typically a person-to-business (P2B) transaction, but P2P money transfers are also available.

To make a P2P transaction, registered users can login to PayPal and provide the email address of a payee and the amount to be paid. The recipient receives an email that the payment has been made. If the recipient does not have a PayPal account, the email will instruct them on how to create one in order to obtain the transferred funds. Payments can be made in 17 different currencies and in over 100 countries and regions. PayPal also offers PayPal Mobile, a service which allows subscribers to make payments via their mobile phones using short message service (SMS) texts, also known as text messaging. This is described in more detail in the mobile payment section below but basically enables users to make payments by texting PayPal a message that includes an amount to be paid and the payee's mobile phone number or email address.

B. Mobile Payments

In the US, m-commerce is still very much an emerging market and the use of mobile phones in the US as a payment device is considerably lower than in Europe and Asia. There are three ways that mobile phone payments can be made, using near frequency communication (NFC), SMS or wireless application protocol (WAP) technologies.

1. NFC

NFC technology is a two-way wireless connection based on short-range radio frequency technology. Mobile payments relying on NFC require (i) the installation of a NFC chip into the mobile phone to store the user's account information and (ii) readers or POS terminals to communicate with the chip. Account information from a bank, credit or debit card is encrypted and stored on the NFC chip installed in the mobile device, which consumers tap or wave at a POS terminal. The POS terminal emits a short-range radio signal that powers the chip on the mobile device. NFC only works at a short distance so the devices can be no more than a few centimeters apart. Once the wireless connection is made between the two devices, payment information or other content can be exchanged. The readers can be installed at POS locations, signs, poster or other media. NFC mobile payments are not yet used by the general public in the US but several targeted trials have recently been completed with positive results and still more are being conducted today.

2. SMS

Unlike NFC, SMS payments can be made anywhere and do not require a reader or POS terminal. However, even though a consumer's phone may have SMS functionality, the user

must still set up an account with a MPSP and register a bank account, credit card, debit card, or prepaid card with that MPSP. To make a payment by SMS, the payer begins by texting a code or command to the MPSP, such as PayPal, with the dollar amount and the receiver's mobile phone number. The MPSP sends a message back to the payer requesting a PIN. The payer must confirm the transaction by entering the PIN. Once the MPSP receives the PIN, the funds are transferred to the receiver's third-party account. The MPSP sends the payment information notice to the receiver, which is received almost immediately. The receiver can move the funds to a bank account or request a check be issued. P2P payments by SMS are gaining in popularity and an estimated \$103 billion P2P payments are traded annually in situations as common as splitting a restaurant bill or repaying a friend.⁷

3. WAP

WAP is a network architecture for content delivery over wireless networks and allows users to browse the internet using their phones or PDAs. While WAP includes the concepts of browsers, servers and URLs, it is intended for small mobile devices such as cell phones, pagers, and PDAs. Because these devices have smaller screens and other limitations, the web content that is developed for WAP is much simpler than what would appear on your desktop or laptop.⁸ To make a mobile payment using WAP technology, the mobile device is used to access information, usually on the internet, via wireless communication. If using a web browser, the user accesses a WAP website and payments are handled the same as traditional online purchases by providing contact and payment information. Some WAP-enabled phones already have purchase applications downloaded onto them. Users can then select the content they want, such as ringtones or video games, and complete the transaction as instructed. Typically, charges appear on the next monthly mobile phone bill. Most Americans are not yet using their phone to go online. In June 2006, a few as 34.6 million U.S. mobile subscribers (16 percent) accessed the internet from a wireless device.⁹ However, the numbers are increasing and mobile content sales are brisk. Qpass, a major supplier of mobile content billing services for mobile carriers, has processed over \$1.5 billion of mobile content purchases since its launch in 2003¹⁰ and, in 2005, ringtones generated \$600 million in sales.

III. Regulatory Framework in the US

Although PayPal is widely perceived as a new payment system, it is really only a new twist on existing payment systems. Its users must have a bank, credit card or debit card account, which PayPal relies on to fund payments made on behalf of its users. Mobile payments using SMS, NFC or paid through a WAP website also use traditional methods. Therefore, these services are subject to existing laws applicable to the traditional payment methods.

A. Regulatory Framework

1. Truth in Lending Act

In the US, credit cards are governed by the federal Truth in Lending Act of 1968 (TILA) and its implementing Regulation Z promulgated by the Federal Reserve Board. TILA and Regulation Z limit a credit cardholder's liability for unauthorized use to \$50. This \$50 liability can only be imposed in transactions where the card issuer has provided a means to identify the

Schnader Harrison Segal & Lewis LLP

New York, Delaware, Pennsylvania, California, Washington, DC, New Jersey

www.schnader.com

authorized cardholder on the account. Therefore, in internet transactions, where a card is not presented to the merchant, cardholders cannot be held liable for any unauthorized transaction amounts. Cardholders may also withhold payment pending resolution of a dispute and assert any all claims (except tort) claims and defenses against the card issuer that it has against the merchant. Also, a cardholder incurs no liability from the unauthorized use of a credit card except as provided in the TILA, so a merchant's claim that a consumer is liable under any other law would be preempted.

2. Electronic Funds Transfer Act

In the 1970s, banks and financial institutions began to offer electronic funds transfer services through automated teller machines (ATMs) and the use of debit cards at POS terminals.¹¹ In response, the Electronic Funds Transfer Act (EFTA) of 1978 and Regulation E were passed to protect consumers by providing error resolution procedures, limiting consumer liability, and requiring disclosure of terms and conditions. Regulation E governs electronic funds transfers (EFTs) made by consumers, including POS transfers, transfers initiated by debit card transactions (whether or not through an electronic terminal) and debits and credits to a consumer account such as a bank account. Under Regulation E, EFTA applies to any "bank, savings association, credit union, or *any other person* that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services." Regulation E does not provide as much consumer protection as Regulation Z. For instance, consumers' liability for unauthorized charges is also limited to \$50 but only if the consumer notifies the card issuer within 2 days of discovery of the loss of theft of the card. For disputed charges, financial institutions have 10 days to investigate, during which time they do not need to credit the consumer's account. Also, cardholders can challenge an unauthorized transaction but have no right to assert claims and defenses arising in the transaction with the merchant against the card issuer such as the fact that the card was not present.

3. Money Services Acts

Most states have laws governing various forms of nondepository financial services, such as check cashers, money transmitters and currency dealers. The state laws governing money transmitters might also apply to internet payment services providers. Generally, a money transmitter is a money services business that allows customers to send and receive money throughout the United States or anywhere in the world. There is little uniformity in these laws. However, almost all states have laws that require a business to obtain a state license before engaging in nondepository financial services. Money transmitters are also subject to federal regulations to monitor and report certain activity. In 1999, the Treasury Department amended the regulations implementing the Bank Secrecy Act to require that money transmitters register themselves and their agents with the federal government.

4. US PATRIOT Act

The US PATRIOT Act was passed after the September 11 terrorist attacks to strengthen money laundering defenses and help the government in its war against terrorism. Of particular relevance to payment systems, provisions of this act makes it a federal crime to operate a money

transmitter business without an appropriate state license and require money transmitters to monitor transactions.

B. PayPal

For its users that want to fund PayPal payments using credit cards, PayPal established merchant accounts with the credit card companies. These transactions are similar to card-not-present transactions and PayPal is charged an interchange fee per transaction. If funded through a bank or debit account, it is processed through the automated clearing house (ACH) network affiliated with the Federal Reserve Bank and PayPal incurs ACH processing fees. The credit card transactions are subject to Regulation Z and the ACH transactions to Regulation E.

The issue of whether PayPal operates as a bank has been raised by several state regulators. Initially, PayPal allowed customers to leave money in prepaid accounts for use in future transactions. Several states sent letters to PayPal questioning whether this arrangement constituted PayPal engaging in banking activities without a license. As a result, PayPal began offering users the option to invest balances in a PayPal Money Market Fund and any funds not deposited in the PayPal Money Market Fund are pooled with other customers' funds and deposited in a bank account at one or more FDIC-insured banks. Initially, these funds had been placed into PayPal's corporate account but now were placed into accounts that PayPal had no authority to withdraw for corporate purposes, derives no economic benefit from and are not carried on PayPal's balance sheet. PayPal also changed its standard User Agreement for PayPal Service. In its User Agreement, PayPal describes itself as a third-party payment intermediary and agent and states, "PayPal helps you make payments to and accept payments from third parties. PayPal is an independent contractor for all purposes, except that PayPal acts as your agent only with respect to the custody of your funds." The Federal Deposit Insurance Corporation agreed in an opinion issued in 2002 that PayPal was acting as an agent and many states followed and discontinued their investigations into whether PayPal was acting as a bank.¹² Since PayPal acts as an agent for the users' deposits that are held with PayPal and these accounts are FDIC-insured, PayPal must comply with FDIC rules.

After the issue of whether it was a bank was resolved, states became concerned about the lack of regulation over PayPal and began to question whether it was operating as a money transmitter. This prompted PayPal to apply for money transmitter licenses or to request written clarification on this issue from states' regulatory bodies.¹³ Currently, PayPal has licenses from at least 37 states and it appears that the states will regulate PayPal as a money transmitter. As stated earlier, the state laws regulating money transmitters vary and PayPal must comply with these laws if it has a license in that state and federal laws applicable to money transmitters.

C. Mobile Payments

M-commerce is an emerging market in the US and the relationship between the parties and the structure of the payment transactions are still evolving. Based on what has been established to date, m-commerce, like PayPal, also relies on existing payment methods. If a mobile payment is funded through an electronic funds transfer from a consumer's account, the transaction will fall under the jurisdiction of Regulation E and will be governed accordingly. If a

consumer makes a mobile payment using a credit card, the transaction will be governed by Regulation Z. For example, in a NFC transaction, if the account information on the chip is a credit card, then Regulation Z would apply. If a mobile payment service is offered by a wireless carrier, and the charges are placed on the consumer's mobile phone bill instead of charged to a bank, credit or debit account, then the payment would be regulated by the Federal Communications Commission (FCC) rules and regulations, including its Truth-in-Billing Requirements,¹⁴ and state telecommunications regulators rather than Regulations E or Z.

IV. Contractual relationship between parties involved

The contractual relationships among parties to a PayPal or mobile phone payment transaction are not that different from the parties to a traditional payment method, mostly because these alternative payment systems rely on the traditional methods.

A. Between Payor and Payee

First of all, the relationship between the payor and payee is not affected. For instance, in the US, the sale of goods is governed by Article 2 of the Uniform Commercial Code (Sales). This would remain true regardless of whether the sale was conducted over the internet, via mobile phone or in person. Accordingly, the parties are entitled to all the rights and remedies under Article 2, including implied warranties and the ability to sue for damages.

B. Between Payment Providers and Payor or Payee

All payment service providers (PSPs) will have terms and conditions that its users must agree to before using their payment service and these will govern the relationship between them. Terms and conditions accepted through the internet are often referred to as clickwrap agreements because users click on an "I Agree" button to acknowledge their acceptance of the terms and conditions. With the passage of E-Sign and the Uniform Electronic Transactions Act in the US, electronic signatures and electronic agreements are now recognized as having the same legal weight as manually-executed signatures and paper agreements. US courts have held that, so long as they comply with contract law and are not unconscionable, clickwrap agreements are enforceable in the US.¹⁵ The court cases addressing clickwrap agreements, however, did not involve m-commerce transactions, so some degree of uncertainty remains about the validity of such agreements in m-commerce transactions. While reading terms and conditions is not necessarily difficult in a face-to-face transaction or from a screen of a desktop or laptop computer, it is considerably more challenging when the medium employed is a screen smaller than the size of a credit card.

One element that must always be established for a valid contractual relationship to exist is mutual assent to the terms and conditions of the transaction. The parties must be given an opportunity to review the terms and be able to prove their assent to those terms and conditions should a dispute later arise regarding the transaction. The requirements for the formation of a valid contract do not change for alternative methods of payments. Because m-commerce is still relatively new and untested in the US, courts have not yet had the opportunity to examine whether the terms and conditions assented to through a mobile device constitute a binding agreement. The specifics of the relationships among parties to an m-commerce transaction have

yet to be fully explored or defined by the courts. As stated above, however, these transactions are still, at their base, retail transactions, which are bound by standard contract law and/or the Uniform Commercial Code.

V. Risks and Liabilities from Fraud and Crime

A. PayPal

1. Fraud – Identity Theft

Fraud on the internet is often associated with identity theft. Identity theft occurs when someone uses another's personally identifying information, like a name, social security number, or credit card number, without permission, to commit fraud or other crimes. The Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year and the FBI says it is one of the fastest growing crimes. Some claim that these crimes are over-hyped by the media, as the percentage of revenue lost to online fraud is going down and online revenue losses due to fraud were 1.4% of total revenue earned in 2006.¹⁶ Identity theft can happen in many ways but with the internet, it is usually because the storage of the information was compromised. Theft can also occur during transmission, either in transport from the consumer to the PSP or from the PSP to anyone it outsources to handle this information. More often though, the storage of it is hacked into by cyberthieves or physically stolen by an employee. These are threats faced by all internet companies though and not just internet payment service providers. However, because they store financial information, payment service providers are a more appealing target for thieves.

Companies that maintain personal information about customers have a duty to maintain their security protecting such information. When information is illegally obtained from a database without the customer's consent, a breach of that duty may have occurred, and the company that had stored it may be liable to its customers who had their confidential information compromised. As with all aspects of internet-related law, potential tort liability of intermediary companies continues to be explored and developed by courts and commentators on a continual basis. All internet PSPs must ensure that they have adequate security measures to protect their customer's information. Because cyber-thieves are constantly developing new ways to bypass security measures, companies must be vigilant in updating their defenses.

2. Fraud in the Transaction

Fraud can also be committed in connection with the sales transaction between seller and purchaser. For example, the seller may have misrepresented an item or failed to deliver it. [Internet auction fraud was the most reported offense to law enforcement and regulatory bodies in the US in 2006] of what¹⁷ and is one of PayPal's biggest problems.

If a buyer disputes a charge, they can rely on the protections from Regulation Z if a credit card was used or Regulation E if a debit card or bank account funded payments. As explained earlier, if a credit card was used for card-not-present transactions, the buyer's liability for unauthorized charges is zero because the card issuer did not provide a means for the cardholder to be identified. Even if the payment was authorized, consumers using credit cards can withhold

payments if sellers breach. Disputed charges under Regulation Z are charged back to the merchant, known as chargebacks, and are one of the biggest problems in internet transactions. Two common reasons for chargebacks are: (i) the buyer's credit card number is stolen and used fraudulently, or (ii) buyer makes a purchase, but believes that the seller has failed to fulfill its side of the agreement (for example, seller did not ship the item, shipped an item that was substantially different from the seller's description, or the item was damaged when the buyer received it). PayPal was assessed substantial fines in 2001 for excessive chargebacks and was faced with the threat of losing its right to continue using credit cards. For the full year ended December 31, 2006, PayPal's transaction loss (including both direct losses and buyer protection payouts) totaled \$126.4 million, representing 0.33% of PayPal's total payment volume.

B. Mobile Devices

Identity theft and transaction fraud are also concerns in m-commerce. As in internet companies, identity theft usually indicates a systemic problem. It may occur when there has been a breach of the security of the platform or system on which consumers' and businesses' information is stored. Also, whether purchasing through SMS, NFC or WAP, there is always a chance that one of the parties may not perform or that an unauthorized charge has been made. There is less of a chance, of course, with NFC POS transactions where one can examine the goods in person and the card and cardholder are present. The risks and liabilities for identity theft and fraud would be the same as discussed in the PayPal section. However, there are usually more parties involved in an m-commerce transaction so there are more points where security can be breached thus increasing the risks.

In order to ensure that losses due to fraud and crime are minimized in an m-commerce world, it is essential that all the participants in the m-commerce process employ the latest technology to ensure that information does not fall into the wrong hands. Handset manufacturers and WAP application developers must operate on the assumption that any existing technology can be hacked. Consumers must be watchful that their cell phones do not fall prey to potential criminals. Most of all, the wireless providers must be vigilant about monitoring their networks. Any compromise to security could lead to public embarrassment and consumer mistrust, potentially leading to a reduction in business.

Additional concerns exist with m-commerce though such as the chance that the mobile device can be lost or stolen or the NFC chip activated by a thief. M-commerce is still in its development stage in the US but some possible security measures include the ability to turn off the payment feature and the requirement of a PIN or biometric identification. Also, unlike Bluetooth, NFC chips have a short range so there is less of a chance that they can be read by thieves.

Conclusion – Looking Ahead

As e-commerce grows, the number of payments made online will too. The pace of growth will accelerate as the younger generations, which are the most comfortable with e-commerce, become tomorrow's primary consumers. Given the different needs and many benefits to consumers and merchants and the potential for profit by providers, multiple options will continue to exist. Financial institutions and non-bank service providers will continue to compete or form

partnerships to position themselves at the forefront of payment industry. Meanwhile, continued investment in risk management will increase consumer confidence but payment service providers must remain vigilant as thieves are persistent and resourceful. Currently, PayPal is leading the way among the alternative payment methods and m-commerce in the US is still low, especially compared to the Europe and Asia-Pacific markets. However, m-commerce and mobile payments are only a logical extension of e-commerce and internet payments, as everything on desktops and laptops is migrating to mobile phones. Capitalizing on the natural relationship between m- and e-commerce will drive future innovations in payments.

Credits

Special thanks to James Levine of Schnader Harrison Segal & Lewis for providing research for this paper.

¹ Source: Pew/Internet

² Although e-commerce sales in the second quarter of 2007 accounted for only 3.3 percent of total retail sales, it increased by 20.8 percent ($\pm 4.6\%$) from the second quarter of 2006 compared to total retail sales which increased by only 3.8 percent ($\pm 0.5\%$) in the same period.

³ Source: Bureau of Economic Analysis, US Department of Commerce

⁴ Source: National Retail Federation

⁵ Source: CTIA – The Wireless Association

⁶ Press Release, PayPal, PayPal Expands to 190 Markets Worldwide (May 10, 2007), *available at* <http://www.shareholder.com/paypal/releaseDetail.cfm?ReleaseID=242097>.

⁷ Becker, *supra* note 7.

⁸ WAP developers use WML and WMLScript instead of HTML and JavaScript.

⁹ Krista Becker, Mobile Phone: The New Way to Pay?, EMERGING PAYMENTS INDUSTRY BRIEFING, Feb. 2007, *available at* <http://www.bos.frb.org/economic/eprg/papers/briefings/mobilephone.pdf>.

¹⁰ Becker, *supra* note 7.

¹¹ JANE K. WINN AND BENJAMIN WRIGHT, LAW OF ELECTRONIC COMMERCE (4th ed. 2007).

¹² Troy Woverton, FDIC decides PayPal's no bank, http://news.zdnet.com/2100-9595_22-858445.html (last visited Oct. 15, 2007).

¹³ Carl Kaminski, *Online Peer-to-Peer Payments: PayPal primes the pump, will banks follow?*, 7 N.C. BANKING INST. 375, 386 (2003).

¹⁴ 47 C.F.R. § 64.2401 (2007).

¹⁵ Hotmail Corporation v. Van\$ Money Pie Inc., No. C-98 JW PVT ENE, 1998 WL 388389 (N.D. Cal. April 16, 1998). This is the first case implicitly holding that a clickwrap contract, specifically a "Terms of Service" e-mail agreement, is valid.

¹⁶ CyberSource.com, Fraudsters Pocket \$3 Billion from U.S. eCommerce in 2006, http://www.cybersource.com/news_and_events/view.xml?page_id=1521 (last visited Oct. 15, 2007).

¹⁷ Source: The Internet Crime Complaint Center