GPayments
Innovate - Empower - Adapt

Authentication and Payment Solutions

Pseudo Card Numbers

A new weapon to combat fraud in eCommerce

At a glance

This whitepaper outlines the concept, benefits and a high-level overview of a pseudo credit card architecture. A number of variations on the basic concept have arisen and it is important to contrast the different approaches to disposable card numbers, single-issue card numbers, pseudo card numbers and virtual credit cards in the market. This whitepaper examines the processes of pseudo card number authentication and integrity matching and the role that these processes can play in authenticating cardholders and reducing fraud in eCommerce. A major aim is to introduce clarity in the market as to the capabilities of current technologies to perform these processes. The whitepaper also covers the benefits of integrating a pseudo card implementation with a digital wallet strategy and the option of providing debit payment capability utilizing existing credit card infrastructure.

Brent Clark
VP Business Strategy
GPayments Pty Ltd
Pittwater Business Park
Suite 8, 5 Vuko Place
Warriewood NSW 2102 Australia

Telephone: +612 9913 3088
Facsimile: +612 9913 3077
Email: brentclark@gpayments.com
Website: www.gpayments.com

While GPayments has taken all reasonable care in preparing this whitepaper, the information, figures and details contained within are presented in good faith. No warranty or guarantee (express or implied) is given by GPayments as to the completeness or accuracy of the whitepaper or any information provided in connection with it.

Pseudo Card Numbers

Background

Online purchases are still perceived as high risk

To date many consumers have been reluctant to provide their credit card numbers over the Internet. This has been a result of a number of high-profile incidents where computer hackers have breached security at online merchants and managed to retrieve credit card databases. It is then possible for these credit cards to be used fraudulently by the hacker as no authentication step is required in online transactions. Credit card security has emerged as the biggest barrier to online purchasing with up to 79 per cent of consumers concerned.[1] It is likely the consumers perception of the risk of using their credit card on the Internet exceeds the reality but nevertheless this has been responsible for slowing the rise of eCommerce. Online retail sales could reach $40 billion by 2002 but this figure could be reduced by almost $18 billion if privacy concerns aren't addressed.[2]

Online fraud is growing

Due to the lack of authentication in online transactions involving credit cards any credit card number acquired by subterfuge in either the online or offline worlds could be used to make online purchases. There have been attempts to introduce authentication protocols such as SET to address this problem. However, the requirement to alter existing websites and the complexity of implementing certificate-based systems for the merchant and consumer has prevented these systems from becoming widespread. It has been estimated that 8 percent of online sales were lost to fraud in 1999. Online fraud is estimated at 10 percent of sales in 2000 rising to 14 percent in 2003.[3]

The pseudo card number solution

Pseudo credit card numbers have recently been gaining a great deal of attention as a new method of combating fraud in online transactions. Consumers are able to apply for a new credit card number when purchasing online eliminating the need to send their real credit-card numbers over the Internet. The purchases made with the pseudo credit card number are recorded against the cardholder's real credit card number by the card issuer following the purchase. Once the newly issued number expires any purchases attempted with that number are invalidated. Pseudo credit card numbers are possibly the easiest fraud reduction system to implement from the perspective of the card-issuer, the merchant and the cardholder.

Benefits for Consumers

Pseudo credit card numbers can be issued to cardholders either at the credit card issuer's website or in a digital wallet provided to the cardholder. This can reduce online credit card fraud from the cardholder as they are required to authenticate themselves when opening their digital wallet or applying for a pseudo credit card number. For example, the cardholder may be required to enter a special PIN number prior to being issued with a pseudo credit card number.

Benefits for Merchants

Merchants do not have to alter their existing website or deploy any further technology to accept these pseudo card numbers. The pseudo card numbers are indistinguishable from real credit card numbers and pass through their existing infrastructure transparently. The merchant does not need to be authenticated in this process as the credit card number stored by the merchant is not

[1] Price Waterhouse Coopers Survery

[2] Jupiter Research

[3] Meridien Research

a real credit card number. Even if a hacker manages to breach security at the merchant's website and retrieve the credit card numbers the pseudo card numbers cannot be used fraudulently if they have expired. Furthermore due to the authentication of cardholders using pseudo card numbers fraud can be reduced. This should address the concerns of merchants where currently 62 percent of online merchants state that fraud is a serious problem.[4]

History of Pseudo Credit Cards

A somewhat similar system was offered in the mid-1990s by a California company, First Virtual Holdings. Consumers had to apply for a First Virtual personal identification number, which was submitted to merchants in lieu of an actual card number. The system did not become popular - those who sought the security may have found the process too cumbersome - and First Virtual abandoned the strategy.[5] A number of companies have recently resurrected this concept and are providing various pseudo card number solutions.

Support from Security Experts

The pseudo card number concept has also gained positive feedback from security analysts. According to Richard Stagg, senior security architect with UK firm Information Risk Management, it is a definite improvement from conventional online credit card transactions.

> "If someone gets hold of numbers from a site, then they are useless….Anything that is one-time is inherently more secure than something that is reused."[6]

Endorsement from major card issuers

Pseudo credit card numbers have already achieved widespread support from major credit card companies. American Express are providing this technology as part of their Private Payments service and Mastercard are pursuing a similar digital identification system which requires PIN codes.[7]

It is in this context that we will now examine the various approaches to pseudo card numbers. This will provide a background for a more in depth analysis of pseudo card authentication, integrity matching and the enabling technologies employed in these approaches.

[4] Mindwave Research

[5] Carol Power, American Banker, 11/4/2000

[6] Will Knight, Zdnet 1/3/2000

[7] Epaynews, "AmEx Offers One-Time Card Number System" 8/9/2000

Firstly, it is important to distinguish between Virtual Credit Card Numbers and Disposable Card Numbers. The focus of this paper will be Disposable Card Numbers but there seems to be some confusion in the marketplace which requires clarification.

Virtual Credit Card Numbers

These are simply real credit card numbers which may or may not have an associated physical card but are guaranteed for online purchases by the card issuer. From a technological perspective there is no difference from a normal credit card transaction as there is no realtime translation or substitution of the credit card numbers during the purchasing process. The credit card issuer is simply taking liability for the cost of transactions when these virtual card numbers are used fraudulently in order to give the consumers confidence to use the virtual card number online.

Examples of these include NextCard Inc., which issues a Visa card that is meant to be used online (but can be used offline). Citigroup Inc. has come out with a MasterCard-branded "virtual credit card" called ClickCredit, which can be used exclusively for online purchases.[8]

Disposable Card Numbers

Disposable card numbers can be broadly segmented into three main groups. Disposable card numbers have evolved as follows:

- **Single-Issue Credit Card Numbers**

  Single-Issue credit card numbers are the most basic form of disposable card number. They are generally issued at a website following application by the cardholder and have identical characteristics as the real credit card number they are mapped to by the card issuer. These credit card numbers expire following a single purchase.

- **Multi-parameter Credit Card Numbers**

  Multi-parameter credit card numbers have evolved additional criteria which make them more flexible than single-issue credit cards. These criteria include:

  - **Card number lifetime**
    This allows the cardholder to request a disposable card number which can be used for a specific period of time before expiring. This may be 20 minutes or 6 months depending on the intended purchasing pattern of the consumer. Multiple purchases can be made using the disposable card number during this period of time. This introduces a higher level of convenience in that the cardholder does not have to apply for a new disposable card number for every purchase.

  - **Transaction value**
    This allows the cardholder to request a disposable card number with a specific credit limit. If a cardholder is about to make a purchase and they know the value of that transaction they are able to use a disposable card number tailored to the particular transaction. This transaction value specified must be smaller than or equal to the credit limit on the real credit card it is issued against.

  - **Number of transactions**
    This allows the cardholder to specify the number of transactions which may be made with a disposable card number. A consumer might know that they want to make three transactions on the Internet and can request a disposable card number which will expire after three purchases have been made.

[8] Jeremy Quittner, "Despite Naysayers, Virtual Credit Cards Become Reality" 28/10/2000

Once any of these criteria are exhausted the disposable card number expires and any further transactions against that number will be invalidated. Multi-parameter credit card numbers provide additional flexibility to the cardholder but do not necessarily introduce any further complexity. Their "default" operation is the same as single-issue credit card numbers unless specified by the cardholder.

- **Pseudo Card Numbers**

  Pseudo card numbers extend the capabilities of multi-parameter card numbers to forms of payment which are not credit-card centric such as debit card or loyalty points. These pseudo card numbers can utilize the existing credit card infrastructure as a transport layer for these payments.

  Consumers often wish to make purchases using their savings account rather than credit account but at present there is no standard for accepting debit card payments over the Internet. It is possible to issue a pseudo card number, which has the same characteristics as a credit card number, but actually results in a deduction from the consumers' debit account or even an accrued surplus of loyalty points. This pseudo card number can be entered into any website which accepts credit card numbers without the merchant having to make any changes. It is then carried transparently as a credit card number to the issuing bank at which point it is translated to a debit card instruction. These card number payments which undergo a metamorphosis in realtime have been dubbed "virtual payment instructions".

Pseudo card authentication and Integrity Matching

Pseudo card authentication is a process initiated between the consumer and the card-issuer prior to making an online purchase where the transaction details are communicated to the card issuer. Once the details such as transaction value are passed to the card-issuer they are stored for comparison with the ensuing request to be received from the transaction acquiring bank. When the request for payment is received from the acquiring bank the card-issuer's software intercepts the request and performs integrity matching on the transaction details before subjecting the transaction to the normal authorization process. If the details received from the cardholder in pseudo card authentication do not correspond with the details received from the acquirer then the integrity matching process fails and the transaction is rejected. This adds a pro-active level of fraud protection above the inherent fraud protection in using single-issue card numbers by allowing card-issuers to completely close the transaction loop.

The concepts of pseudo card authentication and integrity matching only apply where details such as transactional value and expiry times can be captured for each pseudo card number. This process could be achieved via a website but would generally require a digital wallet to make the process convenient for the consumer.

Capture of Pseudo Card Authentication details

There are a couple of methods which can be employed in order to capture pseudo card authentication details using a downloadable digital wallet:

- Profile-based "Web-scraping"
- Intelligent "Web-scraping"
- User input

Website profiling is a method of creating a template which maps the structure and layout of a particular website which can later be used by a program such as a digital wallet to interact with the website. Web-scraping is a process similar to "screen-scraping" where information is captured from a web-page and stored on a central server. Pseudo card authentication using *profile-based "web-scraping"* of the transaction details is possible as a digital wallet knows exactly where the transaction value will be presented in the websites' shopping cart. However, the limitation in a profiled environment is that there is a high cost in building and maintaining the service and it will not work on the majority of websites, which have not been profiled.

Using *"Intelligent web-scraping"* has the potential to work with a greater number of websites and has a much lower maintenance cost. However, these "intelligent" technologies do not currently produce the 100% reliability expected from a bank-grade service and should not be introduced as a mandatory step in the transaction process. The inherent limitations in constructing a pre-authorisation process which performs "intelligent web-scraping" on any website are:

- The shopping cart process can be spread over a number of pages and is dependent on each individual vendor. The vendor cannot be relied upon to communicate the transaction details in a common format.
- There is no guarantee that the user will complete a transaction following a population of the online form. A user may choose not to proceed with the transaction or may alter the details manually.
- Merchant sites cannot be relied upon to quote prices on their webpages with a recognizable currency symbol. For example most U.S websites quote prices as $10.00 rather than US$10.00.

While there have been suggestions in the market that it is possible to fully automate the pseudo card authentication process this is not currently possible using existing technologies. To ensure maximum reliability pseudo card authentication details should be captured via *user input* in a digital wallet. This allows the user to quote the transaction value in the currency of the card they are using to make the purchase. This avoids the multi-currency problem encountered with profile-based "web-scraping" or "intelligent web-scraping technology.

Integrity Matching Criteria

Integrity matching is performed between the transaction details received from the cardholder's digital wallet and the transaction details received from the acquirer to add an optional level of fraud protection.

Information which is not part of the standard messaging protocol utilized by acquiring institutions should be avoided in the Integrity Matching process to ensure maximum interoperability with current eCommerce infrastructure. This information is generally limited to cardnumber, expiry date, transaction amount, transaction date and transaction time.

Transaction matching based upon non-standard data such as merchant details and merchant URL is not possible as current acquiring systems do not provide any facility to send merchant URL's to issuing institutions. Furthermore, introducing variables such as identical date and time in the integrity matching system precludes the customer from making successful purchases at websites which do not do realtime credit card transactions. Many websites do batch processing of transactions or do not charge credit cards until the product ships which may incur delays between the transaction being registered by the consumer's digital wallet and the transaction being processed by an acquirer.

Integrity matching is effectively limited to the transaction value which can be entered by the user and date/time matching based upon a user-defined expiry date/time. For example, a user can specify that a pseudo card will only be valid for a purchase of US$200 for a period of 20 mins.

This integrity matching process benefits the cardholder from two perspectives:

1) the cardholder can limit the amount of their liability in a fraudulent transaction

2) the cardholder can exploit time to limit the capacity of the fraudulent merchant to execute a malevolent transaction

If a card issuer were to mandate that all Internet purchases must be performed using a pseudo card number which cannot be issued until the user is authenticated in a digital wallet this could open the possibility for a liability shift away from the merchant/acquirer in fraudulent transactions.

Implementation Architectures

Pseudo Card numbers can be implemented in three different architectures.

- Credit Card Organisation centric
- Credit Card Issuer centric
- Third Party centric

The differentiating factor in each is the party which controls the pseudo card number substitution process. The card organisation centric model provides a uniform service to all cardholders under a particular brand with pseudo numbers issued directly from a website.

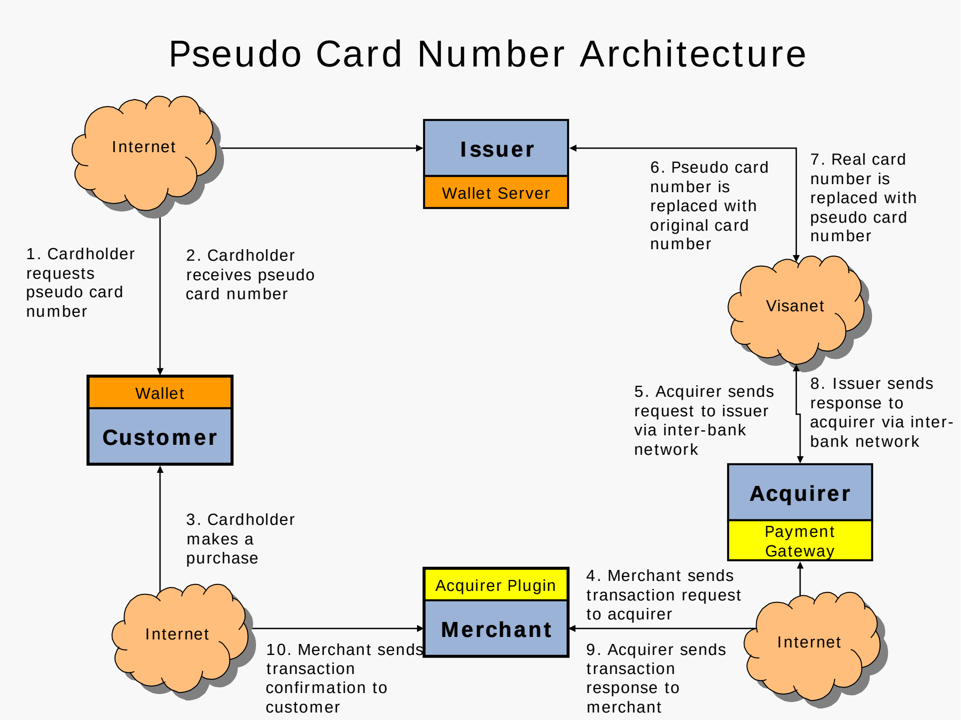
The credit card issuer model gives individual card-issuers (who compete with each other) the opportunity to package pseudo credit card numbers with other services provided by a downloadable wallet for the their cardholder base. This process lends itself to an internal deployment by an individual card-issuer.

The third party model uses downloadable wallet for individuals but provides credit card number substitution in a bureau environment for a number of credit card issuers.

Pseudo Card Number Payment Process

A typical procedure for making a payment using a pseudo card number is illustrated as follows:

- Cardholder requests a pseudo card number using a digital wallet
- Wallet server issues a pseudo card number to the cardholder’s digital wallet
- Customer makes a purchase using the digital wallet
- Merchant sends payment request to the acquirer via an Internet payment gateway
- Acquirer sends payment authorization message to the issuer via an Inter-bank network such as Visanet
- Card Issuer detects a pseudo card number and replaces the pseudo card number with the real card number
- The real card number transaction is authorized in the legacy authorization system
- The Card Issuer substitutes the pseudo card number before sending the response to the acquiring bank
- Acquirer sends transaction response to the merchant
- Merchant sends transaction confirmation to the consumer


Pseudo Card Number Architecture
Internet
Issuer
Wallet Server
6. Pseudo card number is replaced with original card number
7. Real card number is replaced with pseudo card number
1. Cardholder requests pseudo card number
2. Cardholder receives pseudo card number
Visanet
Wallet
Customer
5. Acquirer sends request to issuer via inter-bank network
8. Issuer sends response to acquirer via inter-bank network
Acquirer
Payment Gateway
3. Cardholder makes a purchase
Acquirer Plugin
Merchant
4. Merchant sends transaction request to acquirer
Internet
10. Merchant sends transaction confirmation to customer
9. Acquirer sends transaction response to merchant
Internet

Digital Wallets and Pseudo Card Numbers

The first generation of pseudo card number solutions has been focused on providing the pseudo credit card functionality. However, this has been to the detriment of making the consumer's request and use of the pseudo card numbers simple. For this reason analysts have criticized the Private Payments initiative from American Express for building an extra step into the online purchasing process.[9] The pseudo credit card concept is a sound fraud protection measure, which needs to be made intuitive and transparent to the consumer to increase adoption.

Digital Wallets are programs downloaded by consumers which store a user's personal and financial information such as credit card numbers, shipping and billing address. The first generation of digital wallets were simple PC-based assistants which stored the user's details on a hard disk. The new generation of digital wallets are server-based digital wallets which store the user's information on a central server allowing this information to be accessed by any device connected to the Internet. These new wallets have the capability to perform single-click purchasing at any website using techniques such as "intelligent form population". This is a technology which compares the fields in an online purchasing form against information stored in the digital wallet and uses fuzzy logic in order to automatically populate the order form. Server-based digital wallet systems can simplify the creation and issuance of pseudo card numbers to consumers when they are integrated with a card-issuer's legacy card management system.

The use of a server-based digital wallet can actually improve the current online shopping experience for the consumer by providing single-click pseudo card issuance and then providing single-click online purchasing. Server-based digital wallets can be provided on any Internet-enabled device ranging from the PC to a mobile phone. This means consumers can now access pseudo card numbers for mCommerce transactions anywhere and anytime.

Pseudo Card Numbers and Debit Payments

At present over 95% of online transactions use a credit card as the payment mechanism. However, there is increasing demand for the ability to use alternative payment mechanisms in eCommerce especially in B2B payments where transaction values are generally beyond normal

[9] Gartner: Web Credit Cards 'Are Gimmicks', The Wall Street Journal Interactive, 2/10/2000

credit card limits. Additionally, many consumers would make use of a facility which allows them to access their debit or savings account in order to make online payments.

For a proprietary debit payments system to become universal on the Internet it would require every B2B exchange and every online merchant to implement customized software modules. However, all these websites currently accept credit card payments which has become the de-facto format for making online purchases. Pseudo card numbers are 16 digit numbers created in the likeness of a credit card number which can be entered into existing websites which accept credit cards and are indistinguishable from real credit card numbers by the accepting merchant. Once these pseudo card numbers are received by the card issuer they can perform a payment authorization process from the customer's debit account rather than from their credit account.

The first proprietary online debit payment system has been introduced by the NYCE. However, this "SafeDebit" system requires the user to apply for a physical CD-ROM which then needs to be inserted in their computer every time they wish to make a debit transaction. Every merchant that wishes to accept debit payments using the SafeDebit system must alter their shopping cart in order to accept PIN numbers from customers. This system has not been viewed favourably by analysts:

> Les Riedl, a senior vice president at Speer & Associates, an Atlanta consulting firm, said the crucial question is, "Who will issue SafeDebit?" The potential for lower fraud losses could interest merchants, but banks may have a hard time finding a revenue stream, he said.[10]

The other major area of focus for debit type payments involves using smart cards and/or proprietary smart-card readers connected to a user's personal computer. Both these methods are personal computer centric and do not cater for the explosion in mobile devices which are predicted to become the most common Internet access points.

Pseudo card numbers make these proprietary online debit payment systems redundant by utilizing existing credit card infrastructure in order to carry alternative payments over the Internet. When pseudo card numbers are issued in a digital wallet it is possible to provide a bank-grade security offering entirely in software without any need for proprietary CD-ROMs or smart-card readers. Server-based digital wallets are now accessible on a range of Internet devices making pseudo card number debit payments an mCommerce reality. It is possible that pseudo card numbers and pseudo card numbers will become a standard feature of server-based digital wallets.

Conclusion

Pseudo card numbers are likely to become widespread due to the lack of effective authentication in online credit card transactions. Not only can they reduce fraud in online transactions but they have the potential to accelerate the rise of eCommerce by mitigating the customer's fear of using their credit card online.

Single-issue card numbers are simply the first evolution of the pseudo card number concept. While the implementations of the single-issue card numbers have been relatively immature to date the enhanced functionality of multi-parameter card numbers and pseudo card numbers are expected to move the concept to the next level. These may be introduced in conjunction with virtual credit card offerings by card issuers. However, as the pseudo card numbers can also be used in the physical world in mail order, telephone order and interactive voice response payments it is likely that pseudo credit card numbers will not be limited to eCommerce transactions.

[10] Matthias Rieker, "NYCE Debit-Pay System Wins HSBC, Citi Support", American Banker, 4/10/2000

The processes of pseudo card authentication and integrity matching are likely to become more attractive to card-issuers as card organizations seek to move the liability for fraudulent eCommerce transactions from the merchant/acquirer to the card-issuer. Card issuers will then be searching for solutions, which allow them to authenticate their cardholders, and it is expected that government legislation will follow to ratify this authentication procedure. This authentication will allow the card issuers to ultimately shift the liability for fraudulent transactions to the cardholder. By making credit card purchases PIN or password protected they can be made the responsibility of the cardholder.

Technologies based upon website profiling have not been effective due to the explosion in the number of websites and the constant need to update an existing library of profiles as websites change their layout and structure. The lack of standards in current website shopping cart processes makes it difficult to introduce intelligent technologies for pseudo card authentication and integrity matching. In the medium term the capabilities of current technologies to perform these pseudo card authentication and integrity matching processes will be primarily via user input. This can be streamlined within a digital wallet to make the process convenient for the user.

The implementation architecture for these pseudo card numbers will differ depending on the size and the needs of the card-issuer. However, multi-parameter card numbers and pseudo card number systems, which are integrated with a digital wallet system, are more likely to be deployed internally by credit card issuers. This provides the card-issuer with the ability to provide differentiation in the market through the provision of value-added services. It also gives the card-issuer the capability to data mine their customers online purchases which will be an important resource in tailoring banking solutions to customers needs.

Digital wallets are a complementary offering for pseudo card numbers. Technologies such as intelligent form population offered by a digital wallet can actually improve the purchasing process beyond the normal manual interaction with an online shopping cart. Single click pseudo card generation and single click online purchasing within a digital wallet can make the end-to-end eCommerce payment process simple and intuitive for the customer. Server-based digital wallets can also make pseudo card numbers available for mCommerce transactions on mobile phones and personal digital assistants.

In addition to providing an effective fraud prevention system in credit card transactions pseudo card numbers also open eCommerce to a range of alternative payment methods using pseudo card functionality. The credit card format has established itself as the de-facto standard for payment instructions on the Internet. Pseudo card numbers offer the opportunity to make this format a standard for Virtual Payment Instructions (VPI) ranging from direct debit to loyalty redemption. It also allows existing credit card infrastructure to be utilized for transporting these virtual payment instructions to the correct destination.

Pseudo card numbers will be an effective tool in accelerating eCommerce adoption by consumers and reducing the rapidly increasing problem of online credit card fraud. Pseudo card numbers may actually reach their greatest potential in transforming the way payment is made on the Internet and introducing a variety of new payment methods for eCommerce.

Glossary

Acquirer Financial Institution (or its agent) which acquires from the card acceptor the data relating to the transaction and initiates that data into an interchange system.

Authentication The process of verifying that a party is really who it claims to be.

B2B business to business eCommerce

Cardholder A customer associated with an account, requesting the transaction from a card acceptor.

Digital Wallet A software application that stores purchasing information for the Internet. Such information includes the cardholder's name, mailing address, billing address, credit card number, and often some security information.[11]

Issuer Financial Institution (or its agent) which issues the financial transaction card to the cardholder.

Merchant A merchant offers goods for sale or provides services in exchange for payment. A merchant that accepts payment cards must have a relationship with an Acquirer.

Payment gateway A payment gateway is a device operated by an Acquirer or a designated third party that processes merchant payment messages, including payment instructions from cardholders.

PDA personal digital assistant. A small handheld computer.

PIN A private identification number used by a banking customer to make a payment

VPI virtual payment instruction

[11] Theodore Lacobuzio, Electronic Wallets: The Conceptual Framework October ,The Tower Group 1999