



Global Business Dialogue on Electronic Commerce

Internet Payments

September 14, 2001

Issue Chair	<i>Rijkman W. J. Groenink</i> Chairman of the Managing Board ABN AMRO Bank
Contact Point (Americas)	<i>A. Charles Baillie</i> Chairman & CEO TD Bank Financial Group
Contact Point (Asia/Oceania)	<i>Tatsunori Imagawa</i> Managing Director The Bank of Tokyo-Mitsubishi Ltd.

INTRODUCTION

One of the important issues that will stimulate e-commerce is the availability of easy-to-use and safe Internet payment systems. Internet payment systems will boost volume of sales on the Internet. They facilitate B2B transactions and play a role in the increase of consumer confidence in B2C transactions. A central element in all e-commerce transactions is the presence of trust. The parties to a transaction need to trust each other. They need to trust the system and they need to trust that their privacy is ensured, that their payment will be processed faultlessly and, in the event of a dispute, that they have recourse. In the past the GBDe has actively contributed to the discussion of enhancing trust. During the GBDe Miami Conference in 2000 the GBDe presented work on the development of trustmarks and alternative dispute resolution mechanisms (ADRs), as well

as work on privacy and cyber security. This year the GBDe wanted to examine another important issue for promoting consumer confidence online. The GBDe believes that secure Internet payments are an essential part of trust and consumer confidence.

In the offline world there are many different payment methods. The user has the choice of cash, cheque, money order, debit or credit cards to pay for products or services. In the offline world-in particular- when we talk about micro-payments (i.e. small change) cash is still the preferred payment method. On the Internet credit cards are currently the dominant payment instrument in English-speaking countries. In other countries invoicing, pay on delivery or direct debit is dominant.

In its work on Internet payments, the GBDe has focused its efforts on identifying 1) the current methods of payment on the Internet, 2) describing current and emerging payments technology and 3) attempting to describe the critical elements of any Internet payment method. Based on this analysis, the GBDe also has a number of recommendations for both industry and government on the steps that should be taken to promote and stimulate the (further) development of Internet payments. In this regard the GBDe paper on Internet payments should also be read in conjunction with the GBDe papers on consumer confidence and cyber security.

METHODS OF PAYMENT

The most common e-commerce relationships today are either Business-to-Business (B2B) or Business-to-Consumer (B2C). For e-commerce to succeed, the purchase of goods and services online needs to be easier and faster than today, which means that adequate payment systems need to be developed and used. These payment systems have to ensure that either money is transferred immediately or the customer is identified and the authentication of the payment is guaranteed. In the real world (i.e. off line), cash or pre-paid cards cover the first category and credit cards, debit cards and cheques fall into the second category. In order to adapt these systems to the online environment, a substitute needs to be identified for cash (i.e. an immediate payment that cannot be withdrawn), and the authentication problem for all post-paid systems needs to be solved. Clearly, each system has its specific security issues. Whatever the methods are, it is desirable to complete the whole transaction including payments in a single Website with a high level of security.

I. Business to Consumer Transactions

In analyzing B2C transactions, the GBDe distinguishes among:

1. Systems of prepayment (pay before) such as cash or traveller's cheques or E-Cards and E-Purses;

2. Simultaneous payment (pay now) such as debit card payments with instantaneous settlement; and
3. Systems of deferred payment (pay later or 'post-paid') such as credit card payments, direct debit (the usage of debit cards without a PIN) or simply invoicing.

The major difference among these three types is as follows:

- In pre-paid systems there is no risk for the merchant or for the customer as long as the payment matches with the delivery. Otherwise the user takes the risk that he/she does not get the promised good and the payment cannot be withdrawn. This risk also exists with simultaneous payment types like direct debit. However, the risk is always limited to the amount of (electronic) cash transferred. An advantage of pre-paid systems is that the user may stay anonymous. The usage of pre-paid systems presumes prior money transfer (i.e. buying pre-paid cards or getting cash from an ATM).
- In pay-now systems authentication and settlement have to be made instantaneously, otherwise the bank faces a credit risk. The merchant, however, does not take any risk. The fact that no money has to be transferred prior to the payment is an advantage for the user compared to pre-paid systems. Since access to the user's bank account is essential, we note that the potential risk for the user is higher than for pre-paid systems. Many payment systems, such as debit cards limit the liability to the user but have strict rules regarding the treatment of the card and its PIN code.
- Post-paid systems always come with a credit risk. This risk either remains with the merchant (as in the case of invoicing, direct debits or MOTO-credit cards payment) or the payment service provider accepts the risk (as with credit card payments with a correctly signed receipt) and charges the

merchant for this service. Since the goods are delivered before the actual settlement is done, fraudulent customers pretending to be someone else attempt to abuse payment systems of this type. Therefore, correct identification of the user and authentication of the transaction are crucial.

Based on the foregoing view the GBDe notes that running through an authentication process might be disproportionately expensive when dealing with micro-payments (US\$10 and less). Consequently, pre-paid systems seem to be most appropriate for small payments and in all cases where the user pays a high attention to the protection of his privacy. However, for larger amounts customers prefer post-paid systems (in this case the risk of losing a purse with cash or electronic money plays an important role).

Situation in the different world regions

Availability of payment options varies by region and local commercial custom.

Asia-Oceania

In Japan, cash-on-delivery payments and money transfers are popularly used in addition to credit cards for B2C settlement. Unique to Japan, convenience stores, like 7dream.com run by Seven-Eleven Japan, act as a service provider for e-commerce. Consumers order products online, but pay for (usually in cash) and receive merchandise at convenience stores.

Europe-Africa

In Europe, the payment landscape is heterogeneous. In some countries like France and the UK, cheques still play an important role, in others, such as Germany and Spain, for example, electronic money transfer and electronic direct debit are widely used and come along with low transaction costs. Although chip-based payments cards like the German Geldkarte, Belgian Proton and Dutch Chipknip (a pre-paid e-card system) are already widely available, these systems are still only rarely used. The importance of credit cards differs among the

countries and tends to be most important for cross-border payments - in the real world as well as in e-commerce.

Americas

In North America, in addition to credit cards, which are widely used for B2C payments, banks have targeted Electronic Bill Presentment and Payment (EBPP) as a fundamental application for the Internet and online banking. The benefit to customers is aggregation of their billing data and payments. However, it still has to be seen how customer adaptation develops.

II. Business to Business Transactions

As for B2B transactions, recent estimates suggest that B2B transactions will be 10 times greater in volume over the Internet than B2C transactions by 2003 (Forrester Report, IDC Global Market Forecast and many other reports). Payment options therefore vary given the differences between B2B and B2C transactions. Amounts are generally much larger in B2B than B2C. Fraud concerns therefore are heightened. Consequently several initiatives for secure authentication have been developed for addressing this B2B concern.

The following are recent initiatives designed to address B2B concerns:

1. Identrus LLC was formed by a number of the world's leading financial institutions in April 1999 to create a global trust infrastructure. In addition, Identrus Project Eleanor is now in progress, which covers a global B2B Internet payments solution based on identity verification, by a consortium of Identrus member banks. More information on this initiative can be found on www.identrus.com
2. SWIFT (Society for Worldwide Interbank Financial Telecommunication) is also developing a payment initiation and assurance solution to support bank intermediation in e-commerce. SWIFT is an

industry owned co-operative supplying secure messaging services and interface software to over 7,000 financial institutions in 193 countries. The new e-service SWIFT is developing is called TrustAct & e-paymentsPlus. It provides both identity assurance and payment assurance at every stage along the e-transaction cycle. For further information check www.swift.com

PAYMENTS TECHNOLOGY

The world of payments has always relied heavily on state of the art technology. Only through the use of advanced technology will there be systems that are able to transfer payments at high speed and in a secure environment. The situation is no different for Internet payments. The environment may have changed, the requirements of speed, ease-of-use, and safety have not. Discussed below therefore are the existing and emerging payment technologies, without attempting to favor one over another.

For all post-paid and simultaneous payment systems in B2C and for all B2B payment schemes, it is indispensable to establish the complete confidence regarding each party's identity, to make sure that each transaction is authorized and that both integrity and confidentiality of the payment information is guaranteed.

1. PKI (Public Key Infrastructure)

A PKI is based on public key cryptography. The crucial part of a PKI is the existence of digital certificates issued by a Certificate Authority, which links the public key to the corresponding user. The advantage of a PKI is that it can be used for encryption as well as digital signatures. However, current PKI implementations fall short of multi-party transactions for the following reasons:

- A lack of interoperability in X.509 certificates.
- Businesses or trusted parties must manage hundreds of public certificates on their own.

- Real-time validation of certificates is widely accepted in the application environment, but it is not yet available to the consumer level.
- Further development of legal frameworks is necessary. Worldwide acceptance of digital signatures is desirable in order to reduce the possibility of fraud.

2. SSL (Secure Sockets Layer)

A protocol providing a secure connection over the Internet using public key cryptography. The client must locate the server's public key and then uses this public key to create a session-specific secret key, which it transmits to the server. This secret key is used to secure all messages exchanged between the client and the server for the duration of the transaction (using a fast symmetric encryption scheme). SSL was designed to provide a secure channel between two parties, it does not provide for selective encryption between three parties, as is often required in Internet payments. Obviously, SSL only secures the payment data on its way to the merchant, but the user has no control over what the merchant does with this data. Furthermore, SSL secures only the communication channel. It cannot be used to create signed messages that could be used for non-repudiation purposes. The advantages of SSL are that it is easy to use widely spread and inexpensive. The disadvantages lie in its lack of signed messages and the fact that it has no multi-party security.

3. SET (Secure Electronic Transaction)

This is an open standard developed by Visa International and MasterCard International, among others, to facilitate secure credit and debit cards transaction over the Internet. SET uses digital certificates issued by Certification Authorities and PKI to verify the identity of cardholders, merchants and banks, and to protect payment data from interception. In contrast to the SSL protocol, merchants do not have access to customer's payment card data because card numbers are transmitted in an encrypted form directly to the SET payment gateway. This technique is now already used in so called e-

wallets that are offered by banks in some countries. The clear advantage of SET is that authentication and security are provided; its disadvantage is that its complexity is a barrier to use and it has a relatively high cost.

4. 3D-SET(Three Domain Model)

A simpler version of SET designed to allow issuers a choice of different cardholder security and authentication schemes. It has the advantages of lower cost than SET and interoperability with greater flexibility. Its disadvantage is that it is not accepted worldwide.

5. “Identrus” Model

The technology that is emerging from Identrus is a four-party model, which consists of the concerned parties and their respective related financial institutions. It is being developed especially for the B2B environment. One of the reasons why Identrus is modeled as a four-party model is to minimize the burden of concerned parties. Within the network, the participating financial institutions will act as certificate authorities and issue smart cards holding digital certificates to approved party. This certificate represents a “passport” for engaging in trusted e-commerce. At this moment Identrus and SWIFT are working together. The alliance between Identrus LLC and SWIFT paved the way for an Identrus/SWIFT solution aligning Identrus’ trust model with SWIFT’s Internet-based messaging service, TrustAct.

6. Mobile Technology

In parallel to the development of payment technologies via the Internet there are also a number of technologies being developed for use with mobile telephones. Issues that arise in the development of a mobile payment system are described below.

The mobile payment environment differs quite significantly from the traditional Internet environment because of the following reasons:

1. a mobile phone can be utilized for payment not only in the remote environment (payment over the digital mobile network) but also in the local environment (proximity payments) and in the personal environment (mobile phone linked to PC via local radio link and used for payment during PC browsing session).
2. There is a need for defining and implementing specific mobile payment protocols that take into account the usage mode of mobile phones as well as usability requirements and technology restrictions. Existing Internet payment methods (SET) or local payment protocols (EMV smart cards) are ill suited for the mobile environment.
3. Mobile payment methods currently in widespread use are operator billing (especially for cumulation of small purchases) and unauthenticated credit card payments (mail order-telephone order rules).
4. Mobile payment will start as a complementary, niche payment area: early implementations will concentrate on fulfilling the usability requirements (phone wallets, one-click payments, smart phone covers: initiation of payment transactions via local radio link). Raising the security levels of payment implementations will become more important as the volume grows. Currently there are already some operating systems that are able to authenticate mobile transactions, but services based on these operating systems still need to be developed.
5. With the advent of 3G(third generation) mobile technologies, which are expected to be launched in Europe and in Japan next year, it may not be too long before the mobile device becomes a banking, trading and payments tool, as well as a communication aid. In the longer run, mobile payment will benefit from the global move towards a mobile public key infrastructure.

Critical Elements for Internet Payments

In the previous payment methods and technologies were described. In this paragraph we analyse the critical elements of a successful Internet payment system. The GBDe understands the hesitation of consumers and clients in sending payments over the Internet. By describing the critical elements for Internet payment systems the GBDe hopes to address some of the concerns and contribute to the development of Internet payment systems that not only address these concerns but further encourage e-commerce.

1. Convenience

In order to promote the usage of Internet payment, it is critical to actively promote the use and convenience of payments systems for consumers. Service providers should always examine whether Internet payments cause any inconvenience for users. On the other hand, consumers should realize that certain procedures and tasks involved are indispensable steps in order to protect personal information, even though providing such information seems time-consuming. Internet payments should be available to everyone, anytime and anywhere. The systems employed should be user friendly and easy to understand. If software has to be installed, it should be easy to obtain and be adapted for all existing operating systems.

2. Cost

The cost of use of a payment system (including the set up cost) must be reasonable and should be related to its intended use. Accordingly cost level may differ according to the amount (i.e. micro payments vs. high value payments) and that required extra security for higher value payments may have consequences for the price of the service. The cost of extra security should be optional and transparent to the consumer and business.

3. Transparency

Transparency in the information received by the consumer during the e-commerce transaction, including payment details, is essential. The GBDe 2000 Trustmarks Working Group developed detailed Guidelines for Merchants during the year 2000 that included specific provisions on payments, among others:

- The terms and conditions applicable to the transaction shall include, in the case of using credit or debit cards, the expected time when the card will be charged;
- Prior to the transaction becoming a binding obligation, merchants should provide consumers with a summary that includes the selected payment method.

In addition, it is also essential that consumers know under which conditions refunds will be made for example, in the case of non-authorized transactions and non-delivery of the product.

4. Privacy

Consumer confidence and protection of personal information are indispensable in order to promote Internet based purchasing for consumers. In this context, it is important to make consumers aware of the existence of online trustmark systems and explain easily their usage. It is also necessary to establish policies for the protection of personal information and disclose these to the public. It is desirable to rely on the widely recognized principles regarding the treatment of personal information collected through the Internet. The GBDe 2001 Personal Data Privacy Protection Guidelines constitute an important contribution to enhancing the protection of personal information worldwide.

Privacy considerations should however not prevent an adequate fight against fraud. Exchange of information between operators in the payments markets and the authorities involved is an essential element in any effective fraud prevention strategy. This exchange of

information may involve in certain circumstances a necessary derogation from some data protection principles.

5. Fraud

The great potential of Internet payment systems and, consequently, of e-commerce can be significantly limited by the possibility of fraud. Methods of fraud may range from interception of data to actual hacking into a system. Therefore combating fraud goes hand in hand with the development of Internet payment systems. The prevention of fraud is a task for both industry and governments. An example of government working with industry on fraud can be found in the European Union, where the European Commission published a communication on the prevention of fraud and counterfeiting of non-cash means of payment in February 2001 (COM (2001) 11 final). In this Communication the European Commission recognises the fundamental importance of measures to combat fraud and counterfeiting in non-cash payments by introducing an action plan. The action plan stimulates the close co-operation between public authorities and private parties. It establishes that, although the most important preventative measures are technical, i.e. the use of chipcards, prevention of fraud is most effective if implemented in partnership with all partners, including holders of payment systems, infrastructure network providers and public authorities. Similarly, in the United States, the Federal Trade Commission has established a program of international co-operation to improve investigation and prosecution of fraud in e-commerce.

6. Security

For all post-paid and simultaneous payment systems in B2C and for all B2B payment schemes, it is indispensable to establish the complete confidence regarding each party's identity, to make sure that each transaction is authorized and that both integrity and confidentiality of the payment information is guaranteed. Governments should complete the

legislation to ensure the validity of digital signatures.

The 2000 GBDe Guidelines for Merchants developed by the Trustmarks Working Group recommend that merchants have in place encryption measures that reflect best industry practices for the transfer or receipt of sensitive information, such as personal financial information.

The 2000 GBDe Cyber Security Working Group also made specific security recommendations to all parties in particular in relation to encryption measures and cyber attacks.

7. Liability

All the players involved in e-commerce need to co-operate to establish appropriate rules for allocating responsibility. In addition, it is also indispensable to ensure that users do not suffer losses due to improper use of whatever payment option they choose. However, a distinction should be made between liability in B2B and B2C. In the case of B2B, companies are involved and they should be able to negotiate the distribution of liability themselves. In this respect companies can bear the risks of use of the Internet payment system until the bank has been informed by the customer of loss or theft of the key card or PIN code.

On the other hand in the case of B2C, liability to consumers can be limited, based on system used, as is already now the case, for instance, with credit cards. It is practical for service providers to determine the widely acceptable methods of recovery from damage caused by illegal third-party impersonation.

From the point of view of customer's choice, it is important to maintain the current level of competition between payment methods. It is therefore essential to preserve contractual freedom to negotiate liabilities among the issuing bank, the payment card provider and the merchant. Customers should be informed in a clear and unambiguous way who is responsible for what and under which conditions.

8. Redress

When consumers have problems with their Internet payments, it is essential that appropriate and speedy redress is available. The 2000 GBDe Alternative Dispute Resolution Working Group has developed specific recommendations for dispute resolution including the need for merchants to have specific customer satisfaction systems in place and detailed advice on how ADRs should function.

These Guidelines also recommend that the consumer should address the merchant in the first instance. In the case of payments with credit cards, the merchant may not always be the first instance of redress for the consumer. In line with transparency requirements, consumers should know for each payment method, who they should address in case of problems.

9. Interoperability and Internationality

As reflected in this paper, there are different payment technologies in different regions of the world and that some payment systems are global (in particular those developed by credit card providers). Other payment systems will likely be developed based on regional customs and preferences. This development promotes competition in the market and should not *per se* cause any problem to the consumer. However, to encourage the increase of international Internet payments, those systems need to be able to process payments coming from other systems, even if different. Therefore it is critical to have common and interoperable specifications for the range of Internet payment systems.

RECOMMENDATIONS

The GBDe Working Group on Internet Payments has studied the status and development of both current and emerging Internet payment systems around the world. In this paper we have attempted to describe the main elements of an Internet payment system in a technologically neutral way. The issues that arise are largely of a

technical nature when discussing the set up of an Internet payment system and strongly related to consumer confidence when discussing the operation of Internet payment systems.

For consumers a user friendly and secure payment system is one of the pillars of confidence in e-commerce. The GBDe Working Group on Internet Payments believes that its work on Internet payments should be viewed in conjunction with, trustmarks, ADRs, privacy and security, all of which go to promoting consumer confidence in the Internet. Consequently this paper should be read in conjunction with the work of the GBDe on Trustmarks, ADRs, privacy and cyber security.

The GBDe Working Group on Internet Payments believes that, as e-commerce develops, we will see the emergence of radically new business models as the further development of e-commerce and its inherent cross-border character has implications for a wide range of issues including the delivery of government services, taxing, customs clearance, etc. Internet payment systems will facilitate these developments.

In this context the GBDe would like to make the following recommendations:

- 1) The GBDe encourages payment service providers, e/m-commerce merchants and governments to work to promote the development of Internet payment systems in order that all potential e-commerce customers have –easy- access to at least one payment system that meets their needs, at reasonable cost and convenient. Merchants should inform consumers in a transparent manner of all information related to the payment transaction including available security methods and privacy considerations.
- 2) The GBDe welcomes co-operation of public authorities and private industry in the combating fraud with Internet payment systems. The GBDe urges all parties concerned to work together to develop action plans for the prevention of fraud.

Governments and law enforcement agencies need to pursue legal punishment for attempts of fraud with Internet payment systems. Industry should do its utmost to protect users from systemic fraud with a reliable, secure Internet payment system. Users, however, have an obligation to be cautious with the cards and codes with which they were provided. Moreover, privacy considerations should not prevent an effective effort to combat against fraud.

- 3) The GBDe is committed to working cooperatively with governments and industry to bolster the development and legal recognition of digital signatures in all jurisdictions around the world. The development of digital signatures forms an essential part of the development of a legal regime on the Internet and will be instrumental for the emergence of Internet payment systems. Governments and industry alike need to work on the development of security for digital signatures. Furthermore, governments need to adapt the legal systems to accommodate the use of digital signatures.
- 4) The GBDe urges governments to let parties involved in an Internet payment system chose the conditions, protection and liability of use. Industry must take into consideration measures to protect the consumer. Contract negotiation, in relation to responsibility for fraud or non-delivery, among the different parties involved in a payment transaction is essential to guarantee competition among payment systems. This competition allows the consumer to choose the most appropriate payment method. Although the consumer must be protected against systemic fraud, he must be able to make a rational choice as to the level of protection granted by a payment method. In the case of disputes, consumers should have recourse to easy and speedy resolution. In B2B transactions, liability should always be negotiable between the parties.

- 5) The GBDe does not want to recommend one payment system over another, nor does the GBDe want to promote or prefer global standards to a variety of payment systems. However, for the long term success of e-commerce, we believe interoperability of payment systems is essential. We call on businesses to address, as a matter of priority, the issues of interoperability as they develop their proprietary systems.
- 6) Global e-commerce will naturally lead to more and more cross-border payment streams. Governments must ensure that administrative barriers to cross-border transactions are lowered and businesses must ensure that the growth of Internet payments does not facilitate money laundering.
- 7) All Internet payment service providers should comply with minimum financial regulatory requirements in order to protect consumers. In addition, financial authorities should ensure that new Internet payment providers are supervised in such a way that there will be no risk to the stability of the financial system.