SYSTEM AND METHOD FOR ENHANCING THE SECURITY OF THE BILLING DATA IN VIRTUAL CHANNEL TRANSACTIONS

1. Field of the Invention

The filed of the invention is to enhance the security of the billing data in virtual channel transactions. Especially, it relates to the utilization of a smartcard in the current transaction configuration to enhance the security of the billing data in virtual channel transactions. By this invention, it can lower down the risk in virtual channel transactions and let the consumers trust the virtual channel transaction.

2. Description of Related Art

As computer and network become more and more popular, many business behaviors have already changed tremendously, and the consuming model also has a revolutionary change. The consumers need not to go to physical merchants for shopping or consuming and transform to purchase and pay via various virtual channels immediately. Virtual channels may have the many kinds of forms. For example, it may go through internet (such as: internet merchant, online shopping), telecom network (shopping over telephone, mobile phone), TV-network (such as: TV shopping), or ATM/kiosk/special device allocated at public sites.

However, the communication network is not secure enough. More over, the consumers' billing data might be stolen or leaked out by virtual channel merchants. These situations make the consumers be unable to trust the transaction security of virtual channels. Besides, due to lots of fake cards in the market, some snide consumers might use the stolen credit card on virtual

channel merchants, and it would cause huge loss to the virtual channel merchants and banks. Therefore, although virtual channel transactions are quite convenient, it is accompanied with lots of risks and defects. This inhibits the flourishing of virtual channel transactions.

Recently, because the conventional magnetic stripe credit cards are duplicated or stolen easily, the security of credit card transaction is considered to be enhanced. The financier proposes a smartcard which generally possesses a logic chip to store the cardholder's personal data, such as: name, account number, issuer code, and personal identification number (PIN), etc. The cardholder must use the smartcard and let it be read with a specific reader when he or she makes a transaction. With the higher secure encryption algorithm and processing procedure, the smartcard is therefore more secure than the conventional magnetic stripe card, and it can not be peculated easily. The specification of the smartcard is defined by 3 major credit card organizations: Europay, MasterCard and Visa, and they are being implemented gradually and widely in physical acquiring system. The physical acquiring system architecture of credit/debit card is shown as in Fig.1.

The conventional configuration of internet transaction is similar to that of the physical transaction, except there is a Payment Gateway (PG) allocated at entry of the acquiring system, as shown in Fig. 2, for processing the internet transactions. In conventional virtual channel transaction, only the card account number and expiration date are required in a transaction. However, the defect is that the issuing bank can hardly identify whether the consumer is the lawful cardholder. If the card information is peculated, the virtual channel merchants,

issuing banks and cardholders will suffer the loss and take the high risk.

Because the credit cards with a logical chip embedded (hereinafter as "IC credit card") are deployed and used gradually, the financier is very aggressive to encourage customers to use IC credit card in internet transactions by accessing a personal card reader to read the IC credit card. The IC credit card data will be transmitted to issuing bank for authorization in order to identify that the user does own the IC credit card. However, the process capability of PG with the current technology only accepts user to enter credit card account number and other private information for transaction processing. It can not process the information of IC credit card, nor any function of secure authentication. Hence, conventional internet transaction configuration can not apply in IC credit card transaction directly.

Furthermore, to avoid the credit card data and authentication message from being leaked to the internet merchants, some aware technical solutions, such as: the authentication scheme of Visa "3D Secure", or similarity as of MasterCard "Secure Code", are proposed to let issuing bank be able to authenticate the cardholder directly during internet transaction processing. Nevertheless, the defect of this solution is that the cardholder has to register to the issuing bank in advance. Usually, the consumers own many credit cards from different banks, and they might be issued with new credit cards from other issuing banks very often. If they want to be able to use every credit card they own conveniently, they must register to each bank for every card. This will cause inconvenience, and therefore its popularization of applying is quite low.

To improve the aware technology problem, the inventor delves and proposes the system and method for enhancing the security of billing data in virtual channel transactions, which comprises an acquiring system, a commerce system, and at least one user device. It applies the similar transaction configuration as that is used in physical acquiring system to handle a secure virtual channel transaction. It is only required to build a front end processor at entry of the acquiring system. When a consumer is making a virtual channel transaction, a reader which is connected to the user device is used to read out billing data of the smartcard. The billing data will be specially encrypted and sent to the acquiring system for processing. Although the billing data might go through the commerce system, it can not be recognized what its actual meaning is. Therefore this approach can enhance the security of the billing data. Except this, with the system and method in example embodiments, the consumer can utilize high secure smartcard to make the transaction which will significantly reduce the situations of using the fake credit cards or of peculating credit card data. The risk of virtual channel transaction can thus be lowered down greatly.

Example embodiments can provide the system and method for enhancing the security of the billing data in virtual channel transactions. It is applied to the conventional physical transaction configuration with only building a front end processor at entry of the acquiring system, and therefore the user can use the high secure smartcard in a virtual channel transaction. This will greatly enhance the security of the billing data in virtual channel, and also reduce the situations of using fake cards or of peculated billing data. Herewith

the security in virtual channel transactions can be enhanced.

The system and method of the invention is applied in conventional physical acquiring system configuration by building only one front end processor at entry of the acquiring system, rather than to build a lot of the front end processor systems in all issuing banks for receiving and processing virtual channel transactions. This indicates that it uses relatively low cost to enhance the security of the billing data in virtual channel transactions and reduces the transaction risk of virtual channels.

The user can use the smartcards from many issuing banks but need not to register to them by the system and method. This can increase the user's intention of making virtual channel transaction, so as to boost the usage rate. More over, the virtual channel merchants can still utilize the general virtual channel platform without having to develop an extra system or software. Thus, there is no the extra cost and the handicap for building a virtual channel platform.

The system and method can farther be applied in variant virtual channels for different transaction types. The user can use the various smartcards, readers, networks, and terminals in virtual channel transactions securely, so as to boost the development of virtual channels.

In a first aspect of the invention, there is provided a system for enhancing the security of the billing data in virtual channel transactions, comprising an acquiring system, a commerce system, and at least one user device, wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network, and the commerce system us accessed by the at least one user device to initiate a virtual channel transaction to make an order and sends an activated message to the acquiring system; and characterized in that: a front end processor is set up on the acquiring system transmitting a control component to the commerce system when the acquiring system receives the activated message, so as to the

commerce system transmitting the control component with order data to the at least one user device that initiated the virtual channel transaction; the user device confirms the order data, reads a smartcard by a user device, executes the control component to encrypt the smartcard's billing data, and then sends the encrypted billing data with the order data to the commerce system when it receives the control component; and the commerce system transmits the encrypted billing data to the front end processor, and then the front end processor decrypts the encrypted billing data, transmits it to the acquiring system for payment process, and sends a response message back to the commerce system when the payment process is finalized.

In a second aspect of the invention, there is provided a system for enhancing the security of the billing data in virtual channel transactions, comprising an acquiring system, a commerce system, and at least one user device, and wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network, and the commerce system is accessed by the at least one user device to initiate a virtual channel transaction to make an order and sends an activated message to the acquiring system; and characterized in that: the commerce system transmits a control component with order data to the at least one user device that initiated the virtual channel transaction after the virtual channel transaction is initiated; the user device confirms the order data, reads a smartcard by a user device, executes the control component to encrypt the smartcard's billing data, and then sends the encrypted billing data with the order data to the commerce system when it receives the control component; and the commerce system transmits the encrypted billing data to a front end processor set up on the acquiring system, and then the front end processor decrypts the encrypted billing data, transmits it to the acquiring system for payment process, and sends a response message back to the commerce system when the payment process is finalized.

In a third aspect of the invention, there is provided a system for enhancing the security of the billing data in virtual channel transactions, comprising an acquiring system, a commerce system, and at least one user device, wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network, and the commerce system is accessed by the at least one user device to initiate a virtual channel transaction to make an order, and then sends order data in the virtual channel transaction to the at least one user device and sends an activated message to the acquiring system; and characterized in that: the commerce system transmits the order data to the at least one user device that initiated the virtual channel transaction, and hyperlinks to a front end processor that is set up on the acquiring system; the front end processor transmits a control component to the at least one user device that initiated the virtual channel transaction after hyperlinked; the user device confirms the order data, reads a smartcard by a user device, executes the control component to encrypt the smartcard's billing data, and then sends the encrypted billing data with the order data to the commerce system when it receives the control component; and the commerce system transmits the encrypted billing data to the front end processor, and then the front end processor decrypts the encrypted billing data, transmits it to the acquiring system for payment process, and sends a response message back to the user device when the payment process is finalized.

In example embodiments, the second communication network is the same as the first communication network in the system for enhancing the security of the billing data in virtual channel transactions.

In a fourth aspect of the invention, there is provided a method for enhancing the security of the billing data in virtual channel transactions, implemented by an acquiring system, a commerce system, and at least one user device, wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network; and the method comprising steps of: the at least one user device accessing the commerce system to initiate a virtual channel transaction and the commerce system sending an activated message to the acquiring system; a front end processor being set up on the acquiring system transmitting a control component to the commerce system when the acquiring system receives the activated message, so as to the commerce system transmits the control component with the order data to the at least one user device that initiated the virtual channel transaction; the user device confirming the order, reading a smartcard by a user device, executing the control component to encrypt the smartcard's billing data, and then sending the encrypted billing data with the order data to the commerce system when it receives the control component; and the commerce system transmitting the encrypted billing data to the front end processor, and then the front end processor decrypting the encrypted billing data, transmitting it to the acquiring system for payment process, and sending a response message back to the commerce system when the payment process is finalized.

In a fifth aspect of the invention, there is provided a method for enhancing the security of the billing data in virtual channel transactions, implemented by an acquiring system, a commerce system, and at least one user device, wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network, and the method comprising steps of: the at least one user device accessing the commerce system to initiate a virtual channel transaction to make an order; the commerce system transmitting a control component with order data to the at least one user device that initiated the virtual channel transaction; the user device confirming the order data, reading a smartcard by a user device, executing the control component to encrypt the smartcard's billing data, and then sending the encrypted billing data with the order data to the commerce system when it receives the control component; and the commerce system transmitting the encrypted billing data to the front end processor set up on the acquiring system, and then the front end processor decrypting the encrypted billing data, transmitting it to the acquiring system for payment process, and sending a response message back to the commerce system when the payment process is finalized.

In a sixth aspect of the invention, there is provided a method for enhancing the security of the billing data in virtual channel transactions, implemented by an acquiring system, a commerce system, and at least one user device, wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network; and the method comprising steps of: the at least one user device accessing the commerce system to initiate a virtual channel transaction to make an order; the commerce system transmitting order data to the at least one user device that initiated the virtual channel transaction, and hyperlinks to a front end processor that is set up on the acquiring system; the front end processor transmitting a control component to the at least one user device that initiated the virtual channel transaction after hyperlinked; the user device confirming the order data, reading a smartcard by a user device, executing the control component to encrypt the smartcard's billing data, and then sending the encrypted billing data with the order data to the commerce system when it receives the control component; and the commerce system transmitting the encrypted billing data to the front end processor, and then the front end processor decrypting the encrypted billing data, transmitting it to the acquiring system for payment process, and sending a response message back to the user device when the payment process is finalized.

In example embodiments, the second communication network is the same as the first communication network in the method for enhancing the security of the billing data in virtual channel transactions.

The foregoing and other advantages will be better understood from the following detailed description of preferred embodiments of the invention with reference to the following drawings.

IN THE DRAWINGS

Fig. 1 illustrates the aware technology of the system configuration of physical credit/debit card acquiring system;

Fig. 2 illustrates the aware technology of the system configuration of internet credit/debit card acquiring system;

Fig. 3 illustrates the configuration diagram of one implementation system of the present invention;

Fig. 4 illustrates the configuration diagram of another implementation system of the present invention;

Fig. 5 illustrates the flowchart diagram of one implementation method of the present invention;

Fig. 6 illustrates the flowchart diagram of another implementation method of the present invention.

The following instances are the examples for describing this invention but not to limit the invention.

The invention is mainly designed for virtual channel transactions. It especially applies to but not only the internet shopping, TV shopping, telephone shopping, cable TV network, and the commerce via specific terminals (such as ATM, kiosk, and special device), etc. The main feature of the invention is that the user can use any smartcard issued by any bank to make a virtual channel transactions on a specific terminal. During the processing of the virtual channel transaction, the acquiring system's front end processor in virtual channel transactions will activate a security process by applying a control component to encrypt the billing data that is read from a user's smartcard. Although the user's billing data would go through communication network and virtual channel merchant, it will neither be recognized nor peculated, so as to enhance the security of the billing data.

The system architecture of the invention is shown in Fig.3. It comprises an acquiring system (10), a commerce system (20), and at least one user device (30). The user device (30) communicates with the commerce system (20) via the first communication network (40) to make the virtual channel transactions. The commerce system (20) communicates with the acquiring system (10) via the second communication network (50). In another system architecture as shown in Fig.4, the second communication network (50) is the same as the first communication network (40). That is, the acquiring system (10), the commerce system (20), and the user device (30) communicates in the same communication network (40). The system

architecture of the invention is similar to that of conventional internet transaction system. The main differences are that the acquiring system (10) connects with a front end processor (102), and the user device (30) can execute a control component for encrypting the billing data when the user device (30) makes a transaction by accessing the commerce system (20) and reads the smartcard to get the billing data by a card reader. The above-mentioned first communication network (40) and second communication network (50) can be the wired or the wireless network, such as: internet, local area network, enterprise network, leased line, telecom network, and cable TV network, etc.

In the present transaction system by the physical credit card, the merchant provides a credit card terminal which links to an acquiring bank to read out the data of the credit card and transmits it to the acquiring bank. After primary judgment and verifying, the acquiring bank transmits the data of the credit card to the issuing bank to request for authorization. When having been authorized, the authorized message is sent back to the terminal and then the transaction is finalized. The system configuration of the invention is similar to the description above. However, a control component will be sent to the user device (30) when the user device (30) communicates with the commerce system (20) via first communication network to request to initiate a virtual channel transaction. The control component is executed in the user device (30) automatically to encrypt the data of a smartcard (such as a credit card) that is read by the card reader (302) of the user device (30).

As shown in Fig.3, the commerce system (20) generates an order data and transmits a start message to the front end processor (102) when it starts a

transaction procedure. The front end processor (102) transmits a control component to the commerce system (20) and the commerce system (20) then transmits the order data and the control component to the user device (30). Another application is that the control component is stored in the commerce system (20), and the commerce system (20) transmits the order data and the control component to the user device (30) directly when it starts a transaction procedure. One more instances as shown in Fig.4, the virtual channel transaction is initiated by the user device (30) when it communicates with the commerce system (20) via first communication network (40) to request a virtual channel transaction. The commerce system (20) starts a transaction procedure, generates an order data, sends it to the user device (30), and hyperlinks to the front end processor (102) of the acquiring system (10). The front end processor (102) then delivers a control component to the user device (30) directly via first communication network (40).

When user device (30) receives the order data and the control component, a consumer can confirm the order data via the user device (30), and inserts a smartcard into the card reader (302). Under the control of the control component, the card reader (302) reads out the billing data of the smartcard such as: credit card account number, expiration date, cardholder's personal data, and PIN code, etc, and encrypts them. Then the user device (30) transmits the order data and the encrypted billing data back to the commerce system (20). The commerce system (20) processes the order data and transmits the encrypted billing data to the front end processor (102) which can decrypt it and then transfer it to the acquiring system (10) for payment process. Another

application approach is that the user device (30) can transmits the order data to the commerce system (20) and transmits the encrypted billing data to the front end processor (102) separately, so as to the commerce system (20) can process the order data and the front end processor (102) can process the encrypted billing data respectively and immediately.

The acquiring system (10) has a payment process for the received billing data to verify whether the billing data is valid for finalizing the payment. For example, the acquiring system (10) can be a system to process either physical transactions of credit cards, ATM cards, and stored value cards, or a system with the virtual money account or the e-wallet/e-purse. The billing data can be the information of credit cards, ATM cards, stored value cards, the e-wallet/e-purse, the bank account, the virtual money account, or the account of the agent for the collecting and paying.

The billing data will be verified whether the payment can be finalized. For example, the acquiring system (10) can deliver the credit card data to its issuing bank for authorization, deliver the ATM card data (or banking account data) to the issuing bank for transferring money, verify whether there is enough points or virtual money in the stored value card/virtual money account/e-wallet/e-purse, or connect to the systems of the agent (e.g. telecom company, channel stores) to verify if the bill can be paid. And then, the payment process is finalized means that the credit card has been authorized by the issuing bank, the money in bank account has been transferred, the value in the one of the stored value cards, e-wallet, and the virtual money account has been deducted, or the agent for the collecting and paying has confirmed.

The commerce system (20) can be any kind of system or of platform for the virtual transaction, such as: e-shop on the internet, phone-order system, and TV shopping system, etc. The main function of the commerce system (20) is that it can communicate with user device (30) via communication network (40) to provide a customer to browse and start a transaction flow, and deliver the merchandise or service to the customer when the payment process has been finalized.

The control component can be transmitted to the user device (30) by the front end processor (102) or by the commerce system (20) in according to the start message of the commerce system (20), and it can be an ActiveX software or other designated software, program, or component to control a card reader. The front end processor (102) set on the acquiring system (10) is communicated to the commerce system (20). It decrypts the encrypted billing data, and then forwards the data to the acquiring system (10) for payment process.

The user device (30) which sets up a card reader (302) or links to an external card reader communicates with the commerce system (20) via the first communication network (40). The user device (30) is used to browse and to choose the merchandise or service provided by the commerce system (20), then to start a transaction procedure. The user device (30) can be a personal computer, a notebook PC, a PDA, a mobile handset, a public ATM, kiosk, a shopping device, and a public PC/server, etc. The smartcard can be a IC credit card, a IC ATM card, and a telecom SIM card, etc, which stores the billing data. The personal data of the cardholder might be included in the smartcard too, and

be secured by a high security mechanism. The card reader (302) is a device that can access and transmit the billing data of the smartcard, and it can be an IC card reader, a mobile handset, and a PDA, etc.

In a practical instance, if the virtual channel merchant is an internet e-shop on the internet, the commerce system (20) is the transaction processing system of the internet e-shop. The user device (30) is usually a personal computer, the smartcard may be an IC credit card, and the card reader (302) may be a personal IC card reader. When the user initiates an internet transaction, the internet e-shop can download a control component to the consumer's personal computer to access the personal IC card reader. The consumer inserts an IC credit card into the personal IC card reader, so as to the credit card data of the IC credit card is encrypted and then delivered with the order data to the transaction processing system of the internet e-shop. The transaction processing system then transmits the encrypted IC credit card data to the acquiring system (10) of an acquiring bank, and the acquiring system (10) and the front end processor (102) will take care of the following process.

Generally speaking, different internet e-shops cooperate with different acquiring banks. That is, the different commerce systems (20) usually link to the different acquiring system (10) with different processing procedures, different security mechanism, and different authenticating billing data. Hence, each acquiring system (10) might connect to the different front end processor (102). Another advantage of the invention is that the front end processor (102) of each acquiring system (10) will provide its own control component to the user device (30) via the communication network, when the user device (30) is

making transactions in different commerce system. Because there is little effort for downloading and installing the control component, it will not cause any barrier on the utilization of the invention.

Fig.5 is a flowchart of the method proposed by the invention for enhancing the security of the billing data in virtual channel transactions, which applies to an acquiring system, a commerce system, and at least one user device, and wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network, and the method comprising the steps of :

in step S502, the at least one user device accessing the commerce system to make an order in a virtual channel transaction and the commerce system sending an activated message to the acquiring system;

in step S504, a front end processor being set up on the acquiring system transmitting a control component to the commerce system when the acquiring system receives the activated message, so as to the commerce system transmits the control component with the order data to the at least one user device that initiated the virtual channel transaction;

in step S506, the user device confirming the order, reading a smartcard by a card reader, executing the control component to encrypt the smartcard's billing data, and then sending the encrypted billing data with the order data to the commerce system when it receives the control component; and

in step S508, the commerce system transmitting the encrypted billing data to the front end processor, and then the front end processor decrypting the

encrypted billing data, transmitting it to the acquiring system for payment process, and sending a response message back to the commerce system when the payment process is finalized.

Another application of the above method has the different steps described as following: in step 504,the commerce system transmitting the order data to the at least one user device that initiated the virtual channel transaction, and hyperlinking to a front end processor that is set up on the acquiring system, so as to the front end processor transmitting a control component to the at least one user device that initiated the virtual channel transaction after hyperlinked; and in step 508, the commerce system transmitting the encrypted billing data to the front end processor, and then the front end processor decrypting the encrypted billing data, transmitting it to the acquiring system for payment process, and sending a response message back to the user device when the payment process is finalized.

Fig.6 is a flowchart of another method for enhancing the security of the billing data in virtual channel transactions, which applies to an acquiring system, a commerce system, and at least one user device, and wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network, and the method comprising the steps of :

in step S602, the at least one user device accessing the commerce system to make an order in a virtual channel transaction;

in step S604, the commerce system transmitting a control component

with the order data to the at least one user device that initiated the virtual channel transaction;

in step S606, the user device confirming the order, reading a smartcard by a card reader, executing the control component to encrypt the smartcard's billing data, and then sending the encrypted billing data with the order data to the commerce system when it receives the control component; and

in step S608, the commerce system transmitting the encrypted billing data to a front end processor set up on the acquiring system, and then the front end processor decrypting the encrypted billing data, transmitting it to the acquiring system for payment process, and sending a response message back to the commerce system when the payment process is finalized.

As stated above, the advantage of the invention is that the systems and methods of the invention can significantly enhance the security of the billing data in virtual channel transactions, and lower the situation of forging and peculating the billing data. The above purpose can be achieved in a relative lower cost. More over, the user do not have register to any issuing bank in advance for using any smartcard provided by any issuing bank. The invention has the advantages of high security and excellent practicability both.

In a word, the invention is better than the prior art no matter in the purpose, means, or effect. Nevertheless, please be noticed that the instances above are the examples for the invention only. The scope of the invention will be claimed as follows, and should not be limited to the above implementation instances only. Generally, any decoration or modification in according to the invention, and the combination or separations of the portions and steps in the

invention, should still be contained in the scope of the invention.

CLAIMS

1. A system for enhancing the security of the billing data in virtual channel transactions, comprising an acquiring system, a commerce system, and at least one user device, wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network, and the commerce system is accessed by the at least one user device to initiate a virtual channel transaction to make an order and sends an activated message to the acquiring system; and characterized in that:

a front end processor is set up on the acquiring system transmitting a control component to the commerce system when the acquiring system receives the activated message, so as to the commerce system transmitting the control component with order data to the at least one user device that initiated the virtual channel transaction;

the user device confirms the order data, reads a smartcard by a user device, executes the control component to encrypt the smartcard's billing data, and then sends the encrypted billing data with the order data to the commerce system when it receives the control component; and

the commerce system transmits the encrypted billing data to the front end processor, and then the front end processor decrypts the encrypted billing data, transmits it to the acquiring system for payment process, and sends a response message back to the commerce system when the payment process is finalized.

2. The system as claimed in claim 1, wherein the second communication network is the same as the first communication network.

3. The system as claimed in claim 1, wherein the billing data is the information from one of the group consists of the credit cards, ATM cards, stored value cards, e-wallet, bank account, virtual money account, and account administered by agent for the collecting and paying;

wherein the commerce system is one of the group consists of the TV shopping, telephone shopping, cable TV network, internet shopping, and mobile shopping; and

wherein the payment process is finalized means that the credit card has been authorized by the issuing bank, the money in bank account has been transferred, the value in the one of the stored value cards, e-wallet, and the virtual money account has been deducted, or the agent for the collecting and paying has confirmed.

4. A system for enhancing the security of the billing data in virtual channel transactions, comprising an acquiring system, a commerce system, and at least one user device, and wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network, and the commerce system is accessed by the at least one user device to initiate a virtual channel transaction to make an order and sends an activated message to the acquiring system; and characterized in that:

the commerce system transmits a control component with order data to the at least one user device that initiated the virtual channel transaction after the virtual channel transaction is initiated;

the user device confirms the order data, reads a smartcard by a user device, executes the control component to encrypt the smartcard's billing data, and then sends the encrypted billing data with the order data to the commerce system when it receives the control component; and

the commerce system transmits the encrypted billing data to a front end processor set up on the acquiring system, and then the front end processor decrypts the encrypted billing data, transmits it to the acquiring system for payment process, and sends a response message back to the commerce system when the payment process is finalized.

5. The system as claimed in claim 4, wherein the second communication network is the same as the first communication network,

6. The system as claimed in claim 4, wherein the billing data is the information from one of the group consists of the credit cards, ATM cards, stored value cards, e-wallet, bank account, virtual money account, and account administered by agent for the collecting and paying;

wherein the commerce system is one of the group consists of the TV shopping, telephone shopping, cable TV network, internet shopping, and mobile shopping; and

wherein the payment process is finalized means that the credit card has been authorized by the issuing bank, the money in bank account has been

transferred, the value in the one of the stored value cards, e-wallet, and the virtual money account has been deducted, or the agent for the collecting and paying has confirmed.

7. A system for enhancing the security of the billing data in virtual channel transactions, comprising an acquiring system, a commerce system, and at least one user device, wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network, and the commerce system is accessed by the at least one user device to initiate a virtual channel transaction to make an order, and then sends order data in the virtual channel transaction to the at least one user device and sends an activated message to the acquiring system; and characterized in that:

the commerce system transmits the order data to the at least one user device that initiated the virtual channel transaction, and hyperlinks to a front end processor that is set up on the acquiring system;

the front end processor transmits a control component to the at least one user device that initiated the virtual channel transaction after hyperlinked;

the user device confirms the order data, reads a smartcard by a user device, executes the control component to encrypt the smartcard's billing data, and then sends the encrypted billing data with the order data to the commerce system when it receives the control component; and

the commerce system transmits the encrypted billing data to the

front end processor, and then the front end processor decrypts the encrypted billing data, transmits it to the acquiring system for payment process, and sends a response message back to the user device when the payment process is finalized.

8. The system as claimed in claim 7, wherein the second communication network is the same as the first communication network.

9. The system as claimed in claim 7, wherein the billing data is the information from one of the group consists of the credit cards, ATM cards, stored value cards, e-wallet, bank account, virtual money account, and account administered by agent for the collecting and paying;

wherein the commerce system is one of the group consists of the TV shopping, telephone shopping, cable TV network, internet shopping, and mobile shopping; and

wherein the payment process is finalized means that the credit card has been authorized by the issuing bank, the money in bank account has been transferred, the value in the one of the stored value cards, e-wallet, and the virtual money account has been deducted, or the agent ~~for~~ the collecting and paying has confirmed.

10. A method for enhancing the security of the billing data in virtual channel transactions, implemented by an acquiring system, a commerce system, and at least one user device, wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with

the commerce system via a second communication network; and the method comprising steps of:

the at least one user device accessing the commerce system to initiate a virtual channel transaction and the commerce system sending an activated message to the acquiring system;

a front end processor being set up on the acquiring system transmitting a control component to the commerce system when the acquiring system receives the activated message, so as to the commerce system transmits the control component with the order data to the at least one user device that initiated the virtual channel transaction;

the user device confirming the order, reading a smartcard by a user device, executing the control component to encrypt the smartcard's billing data, and then sending the encrypted billing data with the order data to the commerce system when it receives the control component; and

the commerce system transmitting the encrypted billing data to the front end processor, and then the front end processor decrypting the encrypted billing data, transmitting it to the acquiring system for payment process, and sending a response message back to the commerce system when the payment process is finalized.

11. The method as claimed in claim 10, wherein the second communication network is the same as the first communication network.

12. The method as claimed in claim 10, wherein the billing data is the information from one of the group consists of the credit cards, ATM cards,

stored value cards, e-wallet, bank account, virtual money account, and account administered by agent for the collecting and paying;

wherein the commerce system is one of the group consists of the TV shopping, telephone shopping, cable TV network, internet shopping, and mobile shopping; and

wherein the payment process is finalized means that the credit card has been authorized by the issuing bank, the money in bank account has been transferred, the value in the one of the stored value cards, e-wallet, and the virtual money account has been deducted, or the agent for the collecting and paying has confirmed.

13. A method for enhancing the security of the billing data in virtual channel transactions, implemented by an acquiring system, a commerce system, and at least one user device, wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network, and the method comprising steps of:

the at least one user device accessing the commerce system to initiate a virtual channel transaction to make an order;

the commerce system transmitting a control component with order data to the at least one user device that initiated the virtual channel transaction;

the user device confirming the order data, reading a smartcard by a user device, executing the control component to encrypt the

smartcard's billing data, and then sending the encrypted billing data with the order data to the commerce system when it receives the control component; and

the commerce system transmitting the encrypted billing data to the front end processor set up on the acquiring system, and then the front end processor decrypting the encrypted billing data, transmitting it to the acquiring system for payment process, and sending a response message back to the commerce system when the payment process is finalized.

14. The method as claimed in claim 13, wherein the second communication network is the same as the first communication network.

15. The method as claimed in claim 13, wherein the billing data is the information from one of the group consists of the credit cards, ATM cards, stored value cards, e-wallet, bank account, virtual money account, and account administered by agent for the collecting and paying;

wherein the commerce system is one of the group consists of the TV shopping, telephone shopping, cable TV network, internet shopping, and mobile shopping; and

wherein the payment process is finalized means that the credit card has been authorized by the issuing bank, the money in bank account has been transferred, the value in the one of the stored value cards, e-wallet, and the virtual money account has been deducted, or the agent for the collecting and paying has confirmed.

16. A method for enhancing the security of the billing data in virtual channel transactions, implemented by an acquiring system, a commerce system, and at least one user device, wherein the commerce system communicates with the at least one user device via a first communication network, the acquiring system communicates with the commerce system via a second communication network, and the method comprising steps of:

the at least one user device accessing the commerce system to initiate a virtual channel transaction to make an order;

the commerce system transmitting order data to the at least one user device that initiated the virtual channel transaction, and hyperlinks to a front end processor that is set up on the acquiring system;

the front end processor transmitting a control component to the at least one user device that initiated the virtual channel transaction after hyperlinked;

the user device confirming the order data, reading a smartcard by a user device, executing the control component to encrypt the smartcard's billing data, and then sending the encrypted billing data with the order data to the commerce system when it receives the control component; and

the commerce system transmitting the encrypted billing data to the front end processor, and then the front end processor decrypting the encrypted billing data, transmitting it to the acquiring system for payment process, and sending a response message back to the user

device when the payment process is finalized.

17. The method as claimed in claim 16, wherein the second communication network is the same as the first communication network.

18. The method as claimed in claim 16, wherein the billing data is the information from one of the group consists of the credit cards, ATM cards, stored value cards, e-wallet, bank account, virtual money account, and account administered by agent for the collecting and paying;

wherein the commerce system is one of the group consists of the TV shopping, telephone shopping, cable TV network, internet shopping, and mobile shopping; and

wherein the payment process is finalized means that the credit card has been authorized by the issuing bank, the money in bank account has been transferred, the value in the one of the stored value cards, e-wallet, and the virtual money account has been deducted, or the agent for the collecting and paying has confirmed.

ABSTRACT

The present invention relates to a system and method thereof for enhancing the security of the billing data in virtual channel transactions, which comprises an acquiring system (10), a commerce system (20), and at least one user device (30). The invention applies a similar transaction configuration as that used in physical acquiring system (10) for the virtual channel transactions. It is only required to build up a front end processor (102) at the entry of the acquiring system (10). When making a virtual channel transaction, the customer inserts a smartcard into the user device (30)'s user device (302) and the billing data will be read out, encrypted, and then sent to the acquiring system (10) for processing. Even though the billing data might go through the commerce system (20), it can not be recognized by the commerce system (20). Therefore this will enhance the security of the billing data.

Fig. 5