CHAPTER 3

ELECTRONIC COMMERCE AND ELECTRONIC COMMERCE PAYMENTS

INDEX

3.1 INTRODUCTION.

The objective of this dissertation is the development of an audit approach directed at Internet payment security. An explanation of the relevant concepts related to Internet payment security and electronic commerce is therefore necessary. This chapter will provide a background to electronic commerce and will include the aspects of electronic commerce related to Internet payments. This background is essential to the IS auditor so that a complete understanding of the issues involved will be obtained and so that the importance of electronic commerce will be highlighted. The IS auditor has an important role to play in electronic commerce payment systems. This understanding will then aid the subsequent risk and control identification process. The concepts of risks and controls are introduced in this chapter, and dealt with in detail in Chapters Four and Five, focusing on the risks and controls of electronic payments over the Internet.

"In just a few short years, the Internet has expanded from a limited access academic and research network into a universal, multipurpose electronic medium" (Choi et al, 1999). This aspect will be highlighted in section 3.2.1 below. "In addition to educational and research uses, it has become a popular medium of choice for communicating, advertising and, with the advent of the World Wide Web, for doing business" (Choi et al, 1999). According to PWC (PWCglobal, 1999), "... e-business is the future. It is redefining commerce, transforming industries, and eliminating the constraints of time and distance". This view is also emphasised by the OECD report (OECD, 1999).

Electronic commerce enables businesses to innovate processes from production to customer service by integrating them in a seamless whole. Consumers may search and order products online, exchange product information, learn about product quality from other online users, and negotiate with sellers for lower prices and better quality. Governments are developing electronic commerce platforms to collect taxes, disseminate information, monitor market processes and interact with citizens via personalized, up-to-date communications networks.

According to Choi (Choi et al, 1999) "Electronic commerce has far-reaching implications for the future economy due to the heightened interest among businesses, researchers and government policy makers. Journalists and magazine columnists are making more money on the Internet than are many businesses." Section 3.2.1 below will provide statistics of the success stories related to Internet business. This chapter focuses on electronic commerce and the development of this technology. It is necessary to understand the technology and the aspects around e-commerce so that the background obtained will aid in the identification of the risks and controls involved. This chapter also includes an introduction to electronic commerce payments and a short introduction to risks and control mechanisms around such payments. The risks and controls surrounding e-commerce payments will be discussed in more detail in subsequent chapters.

3.2 ELECTRONIC COMMERCE

3.2.1 ELECTRONIC COMMERCE DEFINED

Electronic Commerce is defined (Cobb, 1998) as "The use of computer networks – the Internet, intranets, extranets, and private networks – to complete business transactions."

Another definition (Martin, 2000) states: "Electronic commerce includes all commercial activities performed through various electronic sources such as the Internet, IT networks, ATM machines, EFT, and EDI, and one of its distinct characteristics is the use of computer to perform the transactions". ISACA (2000) defines e-commerce as "the processes by which organisations can conduct business electronically with their customers, suppliers, and other business partners, using the Internet as an enabling technology". This "does not include existing non-Internet E-commerce methods based on private networks, such as EDI and S.W.I.F.T."

The issues involved in Internet commerce affect large and small companies. As of January, 1996, "half of all businesses with more than 1,000 employees had at least one Web site, according to a Yankee Group survey (which also found that nearly two thirds of all companies with web sites had less than 100 employees)" (Cobb, 1999).

These definitions show that EC basically involves the use of computers to conduct business electronically. This process includes Internet payments, which is the focus of this paper.

To highlight a few examples of the sales of goods and services over the Internet, the US Department of Commerce (1998) quoted the following statistics:

- By the end of 1997, 10 million people in the U.S. and Canada had purchased something on the Web, up from 7.4 million six months earlier.
- 1-800-Flowers sold $30 million online in 1997. While this represents only 10 percent of the company's total revenues, its profit contribution to the overall business is nearly that of its store based business, which is twice as large.
- Amazon.com offers a selection of 2 million book titles to Internet customers (traditional bookstores have about 150,000 titles). In 1996, the company recorded sales of less than $16 million. In 1997, its sales reached $148 million.

This does not only apply to the USA. According to Liang (1999), "...electronic commerce also grows rapidly in Western European countries". Germany Britain and France were identified as "the top three consumer online markets in Europe" and "electronic commerce is also growing rapidly in Australia". "In Asia, although Electronic Commerce revenues are still small compared to the US, it is growing fast".

This view from Liang is also shared by the 1999 OECD report.

The Internet may be attractive to smaller companies because it enables them to reach a wide audience/market with a presence that could be as impressive as that created by much larger entities. According to Cobb, "most major corporations see enough potential to invest significant dollars (over $500,000 per company in the 1,000 employee plus category)." These statistics show that the business over the Internet has experienced phenomenal growth over the past few years. The expectation is that this growth will continue. This highlights the fact that e-commerce is an important factor in business, and the IS auditor must familiarise him/herself with the concepts of e-commerce.

3.2.2 THE HISTORY OF ELECTRONIC COMMERCE (EC)

The following is a brief description of the development of EC according to PWC (1998).

> "Prior to 1997 Web-based EC was not used extensively. There was uncertainty about which products and services should be used to develop commerce sites, to provide Web-enabled content such as advertising or publishing, or to support business activities such as sales or customer service. EC was identified mainly with electronic data interchange (EDI) - an older, less flexible technology that seemed out of step with the new ways of doing business electronically via the Internet."

The use of EDI in the 1980's and early 1990's is also emphasised by EM (1993), as well as ecommerceabout (2000). The further development in the late 1990's (PWC, 1998) was as follows:

> "In 1998, the concept of EC has begun to crystallise in the thinking of most businesspeople. EC enabling tools and technologies – for example, products and services for site development and operations – are recognised as a multi-billion dollar industry in their own right. Perhaps more important, EC is now understood to include the customer interactions of advertising, product selection, contract negotiation, and so on – all the way through to the product and service delivery phase, including logistics, payment, settlement and clearance. As the scope of EC's definition has expanded, the technologies that support EC have expanded as well. The term electronic business was introduced, which includes not only EC but all Web-enabled core business processes, extensive customer integration and connectivity, and strategic transformation of business processes to exploit the efficiencies these technologies make possible."

For many companies, Internet commerce means taking credit card orders from customers or shopping for electronic catalogs on the World Wide Web (ECA, 2000). For others Internet commerce may mean dealing electronically with clients and suppliers, as an alternative to private, leased-line electronic document interchange (EDI over Value Added Networks or VANs). This use of the Internet is sometimes called a Virtual Private Network (VPN) or tunneling. Another area of Internet commerce, which overlaps the two others mentioned here, is digital authentication (of anything from contracts and invoices to photographs).

There are many success stories related to companies that changed their businesses to include electronic commerce activities. These accounts highlight the dramatic growth of Internet business. It also shows that EC has become a very important issue that cannot be ignored by the IS auditor. IS auditors need to understand the concepts and importance of EC so that they will be able to identify the risks associated with conducting business over the Internet, and ensure that these risks are minimised through the introduction of appropriate controls in the business environment.

A few examples have been highlighted in Chapter 1. Below are more examples provided to highlight the importance of EC in business today. According to PWC (1998):

> "Consumer to business Web sites such as Amazon.com and Travelocity.com have attracted extensive media attention as they reach out to a global market, while other chains claim less attention but achieve success: The Disney Store, for example, already sells as much merchandise online as eight physical stores combined. Likewise, Internet portals such as Excite, Yahoo!, and others supported by advertising revenue have experienced rapid and dramatic growth. Through these portals, consumers may shop simultaneously for almost any category of product across many different companies, presenting a radical alternative to mail-order shopping from retailer-specific catalogs or to mall shopping full of stores with unrelated products. However, the majority of investments in technology and most of the transactions occurring over both public and private networks fall into business-to-business category. Firms such as Cisco, Compaq, and National Semiconductor now conduct a significant portion of their business over the Internet."

According to the Organisation for Economic Co-operation and Development (OECD) (1998):

> "The United States is typically credited with about four-fifths of world-wide e-commerce activity. The figures suggest that Western Europe represent about 10 per cent and Asia about 5 per cent of the world total. In Europe, the United Kingdom and the Nordic countries are the current leaders, although some estimates attribute significant activity to Germany. A supporting indicator is the location of the top 100 Web sites for consumer (retail) activity. For each of the major categories of e-commerce activities – live audio, shopping, finance,

> and content (news, sports, adult) – the United States typically has 67 to 85 of the top 100 sites. Canada comes in second for five out of the six categories. Another proxy is the number of adults who access the Internet; the United States accounts for more than half".

Another aspect of EC is electronic 'communities of interest'. The goal of these is supporting and aligning similar organisations in industries such as automobiles, petroleum services, government, and health care. Other communities are also developing that focus on specific business functions, such as purchasing, payments, and human resources, or on personal interests such as investments, books, and travel.

As the above examples illustrate, EC is an aspect that cannot be ignored in today's business world. The indications are that it will grow much bigger than the current situation. It is therefore important for the IS auditor to understand the term EC and to understand what it entails. This is necessary to be able to identify the risks and the role that the IS auditor should play to ensure those risks are controlled by businesses. The next section will explain the various EC categories in the marketplace, and thereafter the two important categories will be examined in more detail.

3.2.3 ELECTRONIC COMMERCE IN THE MARKET

A market consists of (1) market agents including sellers, buyers, intermediaries and other third parties; (2) commodities and services to be exchanged, and (3) market processes such as product selection, consumer searches, competition, marketing and market research, advertising, distribution, payments and consumption. Van der Walt (Van der Walt et al, 1997) also highlights this aspect. In physical markets, consumers visit physical stores, examine products, negotiate, pay and consume physical products. Sellers send out advertisements, collect demand information through various means such as opinion surveys, and distribute their products through wholesalers and retail stores.

In the electronic market, the same market players are engaged in the same economic activities. However, they assume online identities, set up virtual firms and Web stores, communicate, search, advertise and settle payments electronically. The processes of tracking sales, collecting customer information and engineering product specifications not only occur simultaneously, but are integrated to allow real-time feedback. According to OECD (1998) "e-commerce over open networks is a marketplace in which all types of buyers and sellers can interact".

Microproducts and micropayments allow consumers to try out products before paying for a long-term subscription or a large collection. Online usage monitoring along with micropayments enable selling a news report or a magazine column individually but also distributing copyright payments equitably and efficiently. "The electronic marketplace is very similar to physical markets in terms of the economic functions they carry out, but these market innovations can affect the structure of the market and its competitiveness." (Choi et al, 1999). In section 3.2.5 below, the different payment systems are discussed in more detail.

This shows that the basic aspects regarding trading do not change in an EC environment. The difference between 'traditional' business and EC lies in the media used to conduct the business. The underlying technology used in EC changes certain issues and especially in the areas of risks and controls. The risks and controls will be described in subsequent chapters.

3.2.4 ELECTRONIC COMMERCE CATEGORIES

According to PWC (1998): "To succeed, commerce sites targeting consumers need to offer convenience, control, and selection while saving both time and money. Business users have similar needs, but other factors may determine a site's use and success – for example, contractual terms and conditions, availability, or settlement and fulfillment options." The range of EC categories are identified as follows:

- Business to Business (B2B) EC – The use of private networks or the Internet to automate business transactions between companies (PWC, 1998).
- Business to Consumer (B2C) EC – The use of the Internet to sell merchandise or provide services to customers in much the same way as a store or a catalog (PWC 1998).
- Consumer to Consumer EC – Consumers trade amongst themselves with the website offering support and services e.g. online auctions (Hinton, 2000).
- Business to administration (government) EC -- e.g. tax and custom duty, and government and procurement purposes (Liang, 1999).

- Consumer to Administration (government) EC – e.g. welfare payments and personal income tax assessments (Liang, 1999).

The first 4 categories mentioned above are also emphasised by Steinfeld (2000), Ecommerceabout (2001), the European Commission (2000), and Strategis (2001). According to Concord (2000) - "e-commerce refers only to business-to-consumer (B2C) and business-to-business (B2B) selling over the Internet". The differences in these categories are less apparent at the level of the underlying technologies.

It therefore becomes clear that the most common categories being used today are the B2C and B2B categories. The importance of these two categories is also emphasised by Steinfeld (2000), Ecommerceabout (2001), Southcentre (2000), Ecommerce merchant accounts (1999) and Strategis (2001). It is also in these two categories where electronic payments play an important role as a transaction involving buying and selling needs to be completed with a payment. For the purposes of this research, this dissertation will therefore only focus on the first two categories where the focus is on e-commerce payments. B2B and B2C are discussed in more detail below.

3.2.4.1 B2C and B2B EC Categories

Electronic commerce is a very versatile phrase that describes a wide range of activities. It commonly refers to the following (PWC, 1998); (Liang, 1999); (Concord, 2000); (Ecommerceabout, 2001) and (Neiger, 2000):

- searching for product information;
- ordering products;
- paying for goods and services; and
- providing online customer service.

These are commonly referred to as business-to-consumer (B2C) activities.

In addition to these B2C interactions, there are also activities commonly referred to as business-to-business (B2B) activities in electronic commerce. These include

- internal electronic mail and messaging;

- online publishing of corporate documents;
- online searches for documents, projects and peer knowledge;
- distributing critical and timely information to employees;
- managing corporate finance and personnel systems;
- manufacturing logistics management;
- supply chain management for inventory, distribution and warehousing;
- sending order processing information/reports to suppliers and customers;
- tracking orders and shipments;
- making payments.

These activities for B2C and B2B will be discussed again later in this chapter. These online activities are possible because of the enabling technologies which include computer hardware, software, telecommunications networks, and products and processes such as network protocols, encryption programs, real-time applications, digital currency, cyber communities as well as digitized contents available online. According to Choi (Choi et al, 1999), "these enabling technologies are considered to be the building blocks of electronic commerce."

3.2.4.2 B2B Electronic Commerce

Business to business (B2B) EC is divided into several categories. The main ones are

- EDI, in its traditional and web-based forms;
- 'buy-side' procurement applications or systems designed to automate corporate purchasing, particularly for routine, low-value transactions; and
- 'sell-side' catalog-based sites, which in some cases include complex configuration mechanisms to allow customers to configure and price larger, high-ticket orders.

Prior to conducting transactions in the B2B venue, the buyer and the seller typically establish a contractual relationship with each other. This process differs from B2C EC, where a consumer buys from a Web site just by providing a credit-card number. Also, under the current B2B model, the seller usually extends credit to the buyer. The overall effect of the Internet on changes in businesses may also result in changes to the way transactions are initiated and flow through an organisation.

B2B EC activity is typically initiated via a purchase order, a business form (either paper or electronic) that becomes the basis for linking the various processes and stages of the transaction life cycle in both the buyer' and seller's computer systems. The stages of the transaction, linked by means of the purchase order, include origination and processing of the order, delivery, receipt, invoicing, payment, and the related financial recording.

B2B EC products often include (PWC, 1998) "features such as specialised product indexes, parametric searching by product characteristics, and the ability for a purchasing agent to download a catalog for offline searching. These products also support order and billing processes that include customised pricing and the use of purchase orders because most commercial customers buy at negotiated prices and payment terms."

3.2.4.3 B2C Electronic Commerce

According to Neiger (2000) "the most common form of e-commerce is B2C". Prior to EC, there were three B2C models (PWC, 1998): retail stores, direct sales, and mail or phone order (plus a later version of mail order, television shopping);

- Retail stores – In this model, the consumer comes to a place of business (a store) and the supplier's staff are in place, providing a physical environment in which consumers shop and buy. Significant costs are involved in retail stores, including the physical plant, inventory staff, advertising, and so on.
- Direct sales – In this model, the supplier visits the customer's residence. Direct sales effort by door-to-door salespeople and multilevel marketing (often used to sell cosmetics or household items) existed prior to EC, but have only limited relationship to its evolution.
- Mail order – In this model, the supplier and customer transact business without meeting. Mail order, for example, is based on printed catalogs from which shoppers choose their products and either mail, call, or fax in their orders. Mail order may also be costly, but it offers key advantages: it is "open" 24 hours per day, may reach a national or global market without the need for multiple store locations, and is highly flexible.

B2C EC may lower the cost of traditional retail operations. Internet business development is also moving towards new business models that fit the requirements of the consumer. For example, mass marketing is moving to a focus on targeted customer segments and terms such as Customer Relationship Management (CRM) are becoming more common. Other models are developing, such as auction sites, or service providers. This means that specialised forms of business are emerging that fit the business' market objectives by responding to the needs of targeted customers. "Today, most online B2C transactions are conducted using credit cards" (PWC, 1998); Potter, 2001).

The background on B2B and B2C above shows that payments are an essential element of both categories. This dissertation focuses on the payment process and the security around payments for Internet EC. The next section will highlight the payment systems for EC.

3.2.5 ELECTRONIC COMMERCE PAYMENT SYSTEMS

For EC to work, effective methods for paying for goods and services are necessary. This paper focuses on the risks and controls around Internet payments and the following section therefore provide background information for different payment systems. This will aid in the future analysis of the risks and controls around the payments. According to PWC research (1998), three payment methods are emerging.

1. Processes that use existing credit-/debit-card models – Card payment schemes provide a payment mechanism through the secure use of the existing credit- and debit-card payment infrastructure.
2. Electronic funds transfer using a cheque metaphor – A digital cheque is an electronic representation of a cheque; instead of being written on paper, it is digitally created, signed, and delivered. Like a paper cheque, a digital cheque is an instruction to the account holder's bank to transfer funds to a third party upon presentation of the cheque. It uses the existing interbank clearing process for cheque payments and settlements, operates in the same legal framework as its paper counterpart, and with the appropriate software, in principle may be used with current bank cheque accounts.
3. Electronic monetary alternatives – Electronic or digital cash is an electronic replacement for paper currency and coins. It provides the ability to transfer

value, in the form of digital tokens, between a buyer and a seller in exchange for goods or services, ideally without an intervening third-party validation and clearing of each transaction. Either cryptographic authentication or tamperproof hardware (such as a smart card) is required to prevent double spending or counterfeiting. Digital cash will be covered in more detail below.

According to Kabay (1998) "the buying public are leery of engaging in electronic commerce largely because they worry that their electronic transactions will be insecure. Observers in the growing field of e-commerce concur that lack of consumer confidence is the key stumbling block to continued growth of business on the World Wide Web." This aspect is also emphasised in the studies by the Singapore government (Singapore government, 1999), and Ecommerceabout (2001).

3.2.5.1 Online Payment Risks

Although the issues around risks and controls for EC payments will be discussed in the next few chapters in detail, some background information is presented below as an introduction. The problem of Internet security is in principle quite simple because an Internet connection potentially exposes a previously secure system to the world. The issue is not about having a Web site through which external users access a company system. The problem is simply being connected to the Internet at all. An Internet connection is a gateway to the external world, through which anyone with Internet access may attempt to break into an internal computer system. The issue to resolve is how to admit legitimate visitors and keep others out.

All security issues, and the attendant business risks, come together over the issue of online payment. Because of the inherent vulnerability of the Internet, e-business transactions require far more rigorous security to protect confidentiality of the transactions that occur, and of the transfer of high-value assets. According to Garceau (Garceau et al, 1998) "today the most common form of payment on the Internet is the credit card". Duquis (Duquis & Staglin, 2000) also shows the role of credit cards as the most common form of payment still in use. Payments through credit cards are of relatively minor concern in B2C Internet commerce because many security problems are solved by credit cards. Credit cards allow spontaneous transactions without the need for individual buyers and sellers to know and trust one another. For security, card users depend on an intermediary such as an issuing bank or credit card company that qualifies individual cardholders, extends them credit, does credit checks and revokes cards for lack of payment, and constantly detects and manages fraud.

If network security is compromised and an improper transaction takes place, the established credit card infrastructure will handle the problem, guaranteeing, for example, that merchants will be paid and that, under certain laws, users are liable for only a limited amount of a fraudulent transaction. Therefore, the current Internet payment system does not introduce any more risk into the payment process than the model that is currently supported by the normal telephone system.

This does not apply to B2B transactions. Because they may involve large amounts of money and may contain highly sensitive corporate data, they need a better security platform than the ones provided with credit card systems. “In the B2B model that currently exists, there is no substitute for the credit card on a wide-scale basis” (Siebel & House, 1999). Today, each time a company seeks a new business partner, it must qualify the buyer or seller, check credit, negotiate terms, set up accounts payable and receivable, and incur the costs of order-taking, invoicing, payment, and collection. It may be an expensive process.

The above sections provide the background for the two most common EC categories. There is a close link between the EC categories and the payment systems in EC e.g., credit cards and B2C commerce. The security around payments is therefore also a critical aspect of EC. The risks around payments need to be identified and addressed through controls so that customers and business partners will be able to do business with an organisation with confidence.

3.2.5.2 Internet Payment Security

Payment security is critical to the success of e-commerce (Baltimore 1999; Hinton 2000; Entrust 1998; Symantec 2000; Ghosh 1997; & Hinton 2000). In examining the developments of payment security, the following are highlighted (PWC, 1998):

> Early EC transactions were conducted using standard e-mail or Web forms to send the buyer’s credit card data to the seller without any special security. As security and privacy issues increasingly became important, the use of encryption and secure payment processes for online transactions evolved. The most popular process in use today uses SSL, developed by Netscape but

now a de facto standard (Ghosh, 1997) for encrypting data sent between a user's browser and the merchant's server. Although SSL initially was perceived as not sufficient for a robust commercial environment, secure transaction methods other than SSL are having difficulty gaining acceptance in the marketplace.

Today the most frequently used EC method (PWC, 1998) is still "a transaction carried out via an encrypted Web session by a buyer who trusts the merchant to provide goods and services as expected." As the level of Internet sales grows, concerns regarding fraud on the part of the buyer or the merchant increase. The two-party transaction with encryption (SSL) may become a three-party transaction, with the third party certifying the identity of the buyer and the seller through techniques that validate and authenticate both parties.

Processes to authenticate participants through the issuance of certificates are provided by protocols such as Secure Electronic Transactions (SET). (Third-party service providers that guarantee the validity of participants is another alternative.) Aspects such as SSL and SET will be covered in more detail in the following chapters, which address the solutions to the risks of EC payment systems.

3.2.5.3 Non-Credit Card Approaches

"Although most online B2C transactions still are conducted using credit cards in some way, payment technologies not based on the credit card model also are evolving for conducting online sales" (PWC, 1998). Other methods receiving attention include electronic cash such as CyberCoins and DigiCash (which may also be stored on an electronic wallet or on a smart card); stored-value (smart) cards such as Mondex and VisaCash; and micropayments.

This dissertation focuses on the risks and controls governing electronic commerce payments. Although the credit card is still the most common form of payment over the Internet, the non-credit card approaches are also being used. Therefore, any study of electronic payments should also include these non-credit card models, so that the background will be complete and these models should be included in the subsequent risk analysis and control identification process. The next section provides background on these non-credit card approaches to electronic payments.

3.2.5.3.1 Digital Money

It is now necessary to provide a short description of digital money and digital cash because the Internet seems to lack a standard form of digital money - some kind of fast, easy, and secure way to let consumers buy and sell electronically. Many merchants' practices, and many popular Internet-based payment systems are still based on credit cards. According to Siebel (Siebel & House, 1999) "a rash of high-profile security issues has caused many people to lose faith with credit card encryption as a truly secure line for electronic payment. Hence the emergence of digital cash alternatives".

3.2.5.3.2 Digital Cash

The alternative to arrangements that link payment to the buyer's existing credit or debit relationship with a bank is digital (or electronic) cash. The idea behind digital cash is that buyers possess tokens that may be exchanged for goods and services. In many cases, these tokens are used anonymously; that is, buyers use digital cash like ordinary cash, and there is no audit trail connecting the buyer to the purchase. This process accomplishes two goals. Firstly, the transaction is less expensive to execute because there is no need to authorise and then process a credit card transaction. Digital cash therefore opens the door for small purchases, such as an issue of an electronic newsletter. Secondly, digital cash approaches protect the privacy of the buyer, who may be reluctant to have an electronic record created of every purchase they make online.

The exchange of digital cash represents the exchange of electronic tokens (Berbera et al, 1997). In an electronic token system, tokens may be stored on a user's card or computer and may be exchanged directly between remote transacting parties. This exchange does not require a fixed network infrastructure and may be accomplished through an intermittent network connection or even a handheld device. According to Siebel (Siebel & House, 1999) "electronic cash replacements have had trouble gaining public mind share. In consummating online transactions, most people still depend, despite all of their protestations to the contrary, on their credit cards".

The conclusion that is drawn from this is that there is a perception that electronic money isn't "real" money. Electronic cash represents nothing tangible except an electronic number, first in a bank account, then as a set of electrons passing along a wire to a home computer, and then as an arrangement of magnetic domains on a hard disk. When a payment is made, signals are sent from the buyer's computer to another computer, and although the buyer's balance is debited, nothing concrete is handled.

Credit cards may then also be classified as not being real money, either. This may also be said of any currency bill that a Treasury Department issues. "All money is a conventional marker of value. It's just that plastic 'money' has been around for decades, and the electronic equivalent is still struggling for general recognition" (Siebel & House, 1999).

There are some advantages of electronic cash over credit cards. Firstly, it operates much like an ATM. A customer withdraws a certain amount and carries it away from the bank. Because a credit card involves a credit transaction, there are a lot of steps in the process, each contributing unavoidable processing fees. E-cash is carried on a computer instead of on a person and is transferred by wires. And because of the minimal processing fees (zero in some cases), even small payments may be made.

According to Siebel: "Each amount of e-cash carries an irrefutable signature from the bank that issued it - a highly secure digital signature. This makes it very difficult if not impossible to counterfeit. Even though each piece of e-cash also carries a unique serial number that only your computer could generate, the bank cannot know what this serial number is and thus can't trace any purchase or payment you make through e-cash back to its source." E-cash is therefore completely anonymous, just like paper money.

Another advantage with e-cash is that it is possible to prove beyond any doubt that a specific payment to a specific party came from a specific person, and only that person. For example, if someone was the source of an e-cash payment to a black marketer or extortionist, this could be absolutely determined with their cooperation and with data from their computer. So replacing paper and coins with e-cash will make life much more difficult for future criminals.

3.2.5.4 Other Non-credit Card Approaches

3.2.5.4.1 Electronic Wallets

A wallet is defined (whatis, 2000) as "a small software program and data that is used for online purchase transactions. Currently, CyberCash allows the consumer to get free wallet software that allows several methods of payment to be defined within the wallet (for example, several different credit cards)." This process works as follows for one of the wallet software products (whatis, 2000).

- "When you order something, the order is sent to the merchant. The merchant (actually, the merchant's server) sends back an invoice and asks the consumer to launch the Wallet in his computer (or to download it quickly if the consumer doesn't have it yet).
- When the consumer selects 'Pay', the software on the merchant server sends a message back to the consumer's PC that activates the "Wallet" software. The consumer selects one of the cards defined in the Wallet and clicks.
- The transaction includes real-time credit card authorization.
- CyberCash says "soon we will incorporate an electronic 'Cash' and 'Coin' system to use for transactions that are considered small for credit cards".

Electronic wallets are used by consumers to validate merchant servers, secure transaction information and payments, and store transaction data. Many EC software vendors have created their own wallets, which may be downloaded free from a merchant site that is using that particular company's server application and are stored on the user's PC. Although an electronic wallet is not necessary for existing EC transactions using SSL, it is a critical component of SET because the SET digital certificate is stored there. SSL and SET were mentioned briefly earlier on in this chapter, but will be discussed in more detail in the following chapters.

Wallet vendors include Netscape, Microsoft, CyberCash, IBM, Sun, and VeriFone.

3.2.5.4.2 Stored-Value (Smart) Cards

Stored value cards (cards that carry a certain amount of virtual cash stored directly on the chip and do not require online verification of that amount) help reduce transaction costs by allowing consumers to purchase low-price items without a credit card and without the merchant needing to verify each transaction. This approach allows users to gain the portability necessary to shop from any device equipped with a compatible smart card reader.

3.2.5.4.3 EC Payment Processors

Credit card transaction processors are critical to the B2C marketplace. A company may create an online storefront, fill it with products, and invite online customers, but the applications themselves cannot process credit cards or provide critical services such as fraud detection. "The key to effectiveness for transaction processors is the integration of their functionality with back-end applications" (PWC, 1998).

3.2.5.4.3.1 Payment Processing Software Vendors

Web merchants are able to ensure that a credit card number submitted to them is valid through a link to the credit card authorisation network. However, this process may be too costly for smaller EC sites. Furthermore, it only guarantees the card number is valid, without guaranteeing the person placing the order is the legitimate cardholder. "Without SET, Web sites have no means of verifying the identity of the person placing the order" (PWC, 1998).

EC sites use a processing service that provides software and has access to the host bank's payment networks to perform credit-card verification. Some representative transaction processing vendors are listed below. Most fraud detection systems currently deployed on the networks of financial institutions rely on a neural network or "fuzzy logic" approach to fraud, allowing the software to capture suspicious transactions.

CyberCash provides both software and transaction processing services; the software is free, and the transaction processing generates the fees (i.e., it collects its fees from the banks processing the credit cards). Because of the volume of bank transactions it handles, CyberCash charges merchants a relatively low per transaction fee. Because all CyberCash transactions are handled over the Internet, merchants do not have to worry about leased lines or dial-up connections to banks, making this an affordable option for companies just getting started in EC on the Web.

CyberSource, another service provider, provides fraud detection using its own technology. It collects more than 30 pieces of data and performs more than 150 calculations, looking at factors such as spending trends, and where the credit card is being issued to produce a weighted score that allows a merchant to accept or reject an order.

Payment mechanisms and the security around payments form the basis of this dissertation. The above examples provide background on the different payment alternatives available. This understanding will be used in the following chapters and will assist IS auditors to understand the Internet payment environment, which in turn will enable them to perform a preliminary risk analysis on the environment. From this risk analysis it is further possible to identify the possible controls to mitigate the risks.

3.3 CONTROL MECHANISMS

Although these are discussed in more detail in Chapter 5, it is necessary to briefly mention examples of the control mechanisms or technologies in use today, to aid in obtaining a complete overview and understanding of e-commerce. This complete overview will then be used in the next chapters to identify the risks associated with EC payments as well as to identify the controls necessary to address the risks. The risks and controls will then be translated into an audit approach, which may be used by the IS auditor involved in the audit of EC payments over the Internet.

3.3.1 ENCRYPTION

It is possible to keep unwanted users outside a company's systems through a coding process known as encryption. If data is sent as unmodified 'clear text', it is harmfully available to anyone who cares to read it, whether it is the intended party or not. If someone is involved in an online transaction and it is sent in clear text, someone could potentially intercept a name, address, and credit card number. But not if it's in code and that's why encryption is used. But encryption, as logical as it sounds, is not without problems. Among them is the issue of government limitations.

The United States government defines what level of security is legal (Garfinkel & Spafford, 1997), and this level is controlled by something quite simple in principle, the size (in bits) of the security key used to encrypt. While it is always a difficult operation to decrypt any encrypted message, the smaller the key, the easier it is to break a code, which means that the 40-bit code is more vulnerable than the 56-bit code.

3.3.2 AUTHENTICATION

In any business transaction both parties need to offer a guarantee of their identities. Sometimes authentication is as simple as providing a password. In e-business, authentication is accomplished in a number of ways, including the use of encryption technologies that perform authentication as well as encryption (Kabay, 1998).

Authentication requires, among other things, a digital 'signature' (Garfinkel & Spafford, 1997). The process begins with a mathematical summary called the 'hash code', which acts as a compressed representation and unique 'fingerprint' of the message. The hash code is then encrypted with the sender's private key attached to the message. When the message is received, the hash code attached to the message is compared to another hash code calculated by the recipient. If the two match, then the recipient knows that the message has indeed come from the sender, that it has not been altered, and that its integrity has not been compromised.

Keys for digital signatures are filed in a public-key directory, made up of individual user 'certificates' that serve to verify identities, like a bank's physical signature cards. A trusted certification authority manages and distributes these certificates, in addition to electronic keys.

3.3.3 ACCESS CONTROL

Access control determines who gets access to a local or remote computer system or network, as well as what privileges are granted when he or she logs on. Access to information may be restricted at the document level by access-control lists, which itemise the resources that individual users are allowed to access. In addition, access control mechanisms may be distributed on the network. The mechanisms do not have to reside on the same host as the Web site. This means that administrators may physically operate the access-control services on a separate host, allowing multiple Web sites to make use of the same access control mechanisms.

Another mechanism being used is 'smart cards', which complement the existing log-on methods. With a reader attached to the client, absolutely secure client/server authorisation is made possible, guaranteeing that the card is trusted. Stealing the card will of course give the holder an additional opportunity to break in, but the combination of a simple PIN number and the card makes unauthorised access much more difficult.

To limit movements of data between companies and customers, companies adopt various security measures to create what is commonly known as a protective 'firewall'. A firewall (Siebel & House, 1999) "can be software, hardware, or a combination of the two. Its principle function is to serve as an application-level gateway, allowing safe external connections to internal applications." Software and application access rules must be defined, and must be unique to a given application. Used correctly (Siebel & House, 1999), "application gateways provide a high level of security and should make it almost impossible for untrusted external users to execute an internal application - such as, for example, a company's accounts receivable software."

The controls mentioned above, encryption, authentication and access control, are essential elements of e-commerce. The fears of users or customers need to be addressed, as they are a limitation to the success of a company's e-commerce ventures. The controls will be discussed in the next two chapters in more detail.

3.4 CONCLUSION

The above discussion on electronic commerce highlights the fact that electronic commerce is a very new technology which will be important to future business and therefore to the IS auditors. There are many aspects to the e-commerce technology that must be understood by the IS auditor. Especially in the areas of electronic payments there are many vulnerabilities that need to be addressed. Auditors must be aware of all the vulnerabilities as well as the controls available to address these risks. The following chapters will provide a deeper insight into the risks and controls available in EC payment systems.