

**Merchants' Guide to Managing e-commerce Risk and
Fraud**

CONTENT

Introduction	1
1. What is e-commerce all about?	3
2. What are the benefits of e-commerce?	4
3. Potential risks faced in setting up an e-business?	
3.1. Risk Implications	6
3.2. Types of Risks	
3.2.1. Security	9
3.2.2. Payment	10
3.2.3. Fulfillment	12
3.2.4. Legal & Regulatory Issues	13
4. Preventive measures to minimise risks	
4.1 How to minimise security risks?	14
4.1.1. Developing a Security & Risk Management Policy	14
4.1.2. Secure Sockets Layer	15
4.1.3. Firewalls	15
4.1.4. Anti-virus Software	15

Merchants' Guide to Managing e-commerce Risk and Fraud

4.1.5. Software patches	16
4.1.6. Network monitoring	16
4.2. How to minimise payment risks?	17
4.3. How to minimise fulfilment risks?	18
4.3.1. Physical Goods	18
4.3.2. Digital Goods	
5.0. Adopting e-business best practices	20
5.1. Communication	20
5.1.1 Business & General Information	20
5.1.2 Product Information	21
5.1.3 Confirmation and Payment Information	22
5.1.4 Fulfilment	23
5.2 Customer Data Management	23
5.3 Security and Risk Management	24
5.4 Regular Monitoring of Transactions	29
5.5 Redress and Dispute Resolution	30
Appendix A – TrustSg Core Principals	31

Merchants' Guide to Managing e-commerce Risk and Fraud

Appendix B – Model Data Protection Code for Private Sectors	34
Glossary	39
Reference List	42

Introduction

The Internet revolution has radically altered the way businesses are conducted. The size and location of a business are no longer relevant as all companies compete on a level playing field in an Internet-connected global village. Businesses have redefined their objectives and strategies to capitalise on the abundant opportunities of e-commerce. New marketing and sales channels have evolved with the Internet age offering businesses better avenues to explore new markets, strengthen customer relationships, reduce business costs and increase sales revenues.

Although globalisation and the Internet have brought enormous opportunities and benefits to businesses, new competitive challenges and risks have also surfaced. Compared to offline businesses, communicating and transacting online makes businesses more susceptible to fraud. The threat of fraud is one of the main reasons discouraging businesses and consumers to go the “e-way”. In order for e-commerce to take off, businesses and consumers have to embrace e-commerce. But most lack the trust and confidence to do so. It is for this reason that the **National Trust Council (NTC)** has developed this “**E-Commerce Risk and Fraud Management Framework**” for **B2C e-commerce merchants**.

The NTC was formed in March 2001 with a mission to build confidence amongst businesses and consumers to spur e-commerce growth in Singapore. Its first initiative was the **nationwide trust mark programme, TrustSg**, which was established to recognise and promote local e-businesses with sound business practices. The **TrustSg Core Principles** covers various areas from accurate and adequate communication to consumers, to integrity in the management of consumer data and putting in place proper dispute resolution procedures. Apart from this framework, merchants can make use of the TrustSg checklist as an added measure to create a more secure online environment for themselves and their customers.

The literature aims to make merchants more aware of the risks involved in running a B2C e-commerce business, and also offers tips on ways to counter such risks. Merchants who will benefit from this framework include:

Merchants' Guide to Managing e-commerce Risk and Fraud

- Merchants intending to embark on e-commerce;
- Merchants who have recently launched their e-commerce operations; and
- Merchants with established e-commerce operations.

1.0 What is e-commerce all about?

Most people today associate the concept of electronic commerce (e-commerce or EC) with using the Internet to market and sell one's goods and services. There are generally 2 kinds of e-commerce: business-to-business and business-to-consumer, or rather B2B and B2C, respectively. In this chapter, we take a closer look at what each kind of e-commerce is about, and how businesses can reap benefits from capitalising on e-commerce usage.

Business-to-Business (B2B) E-commerce

B2B e-commerce, in its simplest form, refers to a company buying from or selling to other companies through electronic means. This means that the communication and/or transaction between both parties are done online. Through the Internet, regardless of size and location, companies can communicate with each other electronically and efficiently.

Business-to-Consumer (B2C) E-Commerce

B2C e-commerce generally refers to a company selling its goods and/or services to customers using the Internet as the communication channel.

What kind of e-commerce to use?

These are the two basic types of e-commerce, but there are countless variations. Companies can choose to employ more than one type for their business operations. Depending on the business nature, objectives, key success factors and target customers, companies can embark on the type of e-commerce that synergises with its overall business strategy.

2.0 What are the benefits of e-commerce?

E-commerce has radically altered the way businesses are conducted. This includes the way goods and services are created, sold and delivered to a customer. E-commerce has also transformed the way a company works with its partners. To understand e-commerce and be able to capitalise on its opportunities can be extremely rewarding for companies. Below are some well-established benefits that companies can yield from e-commerce:

- Improved Productivity and reduced cost

Through e-commerce, businesses can look forward to more efficient and convenient means of communicating and transacting with business partners and customers. Also, human errors can be effectively reduced, wasteful duplications and non-value added tasks such as unnecessary paper work would be eliminated. This saves huge amounts of time and resources, improving speed and accuracy in business operations, and thus escalating productivity. In addition, efficient communication, quicker turnaround time and closer access to markets equate to reduced cost.

- Streamlined Business Processes

Businesses can capture even more cost savings if they take a step further to integrate their internal processes and backend systems with e-commerce. By doing so, businesses can cross-share important information such as sales forecasts, advertising and promotional plans, and point-of-sale data amongst different functions for greater efficiency and more prompt decision-making. Business processes can also be made more efficient with automation for straight through processing.

Merchants' Guide to Managing e-commerce Risk and Fraud

- Taking Customer Service to a New Level

By advancing your business operations to the Internet, customers also enjoy the convenience of easy access to product information, online purchasing and staying in contact with service providers at anytime and anywhere. Businesses can also communicate more efficiently and respond faster to customer needs and queries.

- Vast Opportunities for New Businesses

The Internet can propel a business to the global business arena, giving it maximum exposure and customer reach far beyond its existing markets. This also opens up new business opportunities for strategic alliances with overseas partners. The Internet is an excellent platform for businesses to exploit and expand their markets.

3.0 Potential risks faced in setting up an e-business?

Operating any business is not without its risk, and e-commerce is no exception. In fact, there are some risks that are unique or more pronounced in e-commerce businesses relative to offline businesses. Some of the key considerations for merchants embarking on or already managing an e-commerce business includes the need to differentiate legitimate customers from fraudulent users in real time, establishing an adequate security system to detect and minimise online payment fraud and unauthorised access to network and data. Anywhere along the B2C transaction flow; from the customer entering his/her billing and shipping address, confirming purchase order, making online payment to merchant, to the fulfilment of goods and services, valuable information can be tampered with or stolen, creating opportunities for disputes and fraud. To optimally capitalise on e-commerce technologies, merchants need to first understand the implications of the risks and how they can impact on their businesses.

3.1 RISK IMPLICATIONS

- Loss of merchandise from fraud

The merchant will lose the value of physical goods if such goods are shipped to fraudulent addresses. Also, if the merchant decides to deliver the goods to the buyers via third parties, for e.g. a shipping agent, and also engage them to collect payment on their behalf, they can run into a risk of losing both the goods and monies collected.

- Chargeback costs associated with customer disputes

A chargeback is a transaction that is returned as a financial liability by the credit card Issuer (Issuing bank) to the Acquirer (bank that provides credit card processing facilities to a merchant), and most often, to the merchant. Chargebacks can occur for a variety of reasons, including:

Merchants' Guide to Managing e-commerce Risk and Fraud

- Customer-disputed transactions
- Fraud
- Authorisation issues
- Inaccurate or incomplete transaction information
- Processing errors

Most chargebacks begin when a cardholder notifies his or her Issuer that there is a transaction problem on the monthly billing statement. When this happens, the Issuer may request for more information from the cardholder. Once the Issuer receives the necessary information, the first step is to ascertain whether a chargeback situation truly exists. If the Issuer determines that a chargeback right applies, the Issuer can resolve the disputed transaction by either sending the transaction back to the Acquirer, and crediting the cardholder's account or decide to absorb the loss on goodwill to the customer

Issuers have about 120 days from the transaction date to chargeback the customers' disputed transactions. This means that fraudulent activity can end up posing a significant risk to the merchant long after the transaction has been processed. In the event of a chargeback, the merchant is required to return the money to the customer, and in addition, also incur a chargeback fee to the bank as payment for handling investigation and administrative work.

- Loss of Credit Card Payment Processing Services

Because the credit card is the most popular form of payment mode for B2C e-commerce transaction, it is important for merchants to put in place best practices to minimise customer disputes that may or may not result in chargebacks. If this is not addressed, merchants may have their

“Merchant” status withdrawn and not be able to avail credit card as a payment mode to customers. Sometimes, the merchants may also have to pay bank charges and reimburse the banks for penalties and fines levied by the Card Associations.

- Inhibited business growth

Merchants with insufficient systems security or authentication technologies in place may need to set up work-around solutions in an attempt to minimise risk. Without any authentication means, merchants that deal with new and unfamiliar buyers are exposed to substantial risks of disputes, fraud and ultimately, financial losses. Depending on the type of goods and services sold and the value of the transaction, merchants need to spend extra time and resources to perform ‘exception processing’ to verify the genuineness of the buyer before accepting the orders and delivering the goods and services. Such manual processes are impractical, inefficient and not sustainable in the long run especially when business volume grows.

- Loss of Reputation

The inability to curb hacking (*“Hacking” will be covered in greater details in the section on “Types of Risks”.*) can seriously disrupt business operations resulting in a reduction in sales revenue. Highly publicised customer disputes can lead to severe loss in customer confidence. This can be extremely damaging to a merchant’s business reputation. The negative impacts on businesses can vary from loss of businesses, loss of market share to even legal suits. The cost of damage control, and business and reputation recovery will be astronomical.

3.2 TYPES OF RISKS

3.2.1 Security

Conducting businesses via the Internet, offers many benefits, one of which is the ease of communication between different parties. However, the online mode of communication also runs into the danger of outsiders stealing vital information such as credit card numbers or banking account information or making unauthorised changes to the information. There is thus a pressing need to ensure the integrity of online information exchanges. It is important to be mindful of all the different risks that a security system can be exposed to and take effective measures to overcome or minimise such risks.

- Viruses

A computer virus can be a program or piece of code that is loaded onto a computer. It is able to attach itself to other files and repeatedly replicating itself, often without the user's knowledge or permission. There are numerous ways in which a virus can spread; through an attachment to an email, by downloading infected programs or software from other websites, or through a floppy disk or CD.

While some viruses remain dormant in the computer system unless activated by a trigger, other viruses become active as soon as the infected file is opened. Triggering a dormant virus could be as simple as reaching a particular date or opening an email that would execute the virus program. Many new viruses are created every month, and no computer system is immune to virus attack. The severity of the damage caused varies with the type of virus attack. Some viruses merely reproduce itself without causing further damage. Others are capable of corrupting the information in your system, wiping all the information, causing a system crash and forcing businesses to shut down.

- Hacking

Hacking occurs when an intruder attempts to gain unauthorised access to your computer system. Any computer connected to the Internet is susceptible to attacks if the necessary security measures are not taken.

Hackers are capable of breaking into computer systems causing defacement of websites, system breakdown, disrupting business operations with denial of service attacks. They can also intercept information transmission and steal valuable information belonging to customers. This will lead to a loss in customer confidence and a reduction in sales revenue. E-merchants will need to channel time and resources into damage control and reputation rebuilding.

3.2.2 Payment

The various modes of payment in the e-commerce businesses include offline payment such as cheque and cash, and online payment such as credit card, stored-value cards and online debit via Internet banking. Credit card payment remains prevalent for online transactions because it provides ease and convenience, and can support multi-currency transactions. The most common of these in the Singapore market are Visa, MasterCard, American Express, Diners Club and JCB. The other option available to buyers is the stored-value cards, called NETSCash, which is the use of CashCard on the Internet. In comparison to credit cards, CashCards gives users the benefit of anonymity. Online debits via Internet banking is currently limited to bank-specific accounts, Singapore dollars clearing and Singapore-based merchants.

All types of online payment require buyers to reveal personal information. Payment through credit card requires disclosure of card number, expiry date and personal address. On the other hand, online debit via Internet banking and stored-value card uses ID account and PIN at the bank's Internet site or NETs' website. This potentially puts both the buyer and merchant at risk of dispute and fraud in the transaction of card payment. Some of the risks involved in card

payment include:

- Repudiation

This occurs when genuine cardholders dispute an online transaction. This can arise due to a number of reasons, for example:

- (i) Goods ordered did not reach cardholder
- (ii) Disagreement over the currency conversion rate
- (iii) Goods received not according to customers' specifications

- Account takeover fraud

This occurs when the fraudster assumes the identity of a legitimate cardholder by obtaining their card and/or billing address details. These can be obtained either from card receipts or numerous 'hacker' sites, which publish lists of stolen card numbers and billing details

- Card Generators

Card generators are software programs that can be found on the Internet, which are able to randomly generate or extrapolate card numbers. These programs will typically also generate a card expiry date. Fraudsters may attempt to use these information to purchase goods online, even though there is no guarantee that such information i.e. account number and/or expiry date produced by these tools are valid.

- Changing shipping addresses

Shipping addresses can be altered after a valid transaction has been made. A fraudster hacks into the merchant's order system, then assumes the identity of an authentic customer and illegally requests a change in

the shipping address.

- **Lost and Stolen Cards**

In this scenario, the consumer's card is stolen and used to make a purchase on the Internet before the card owner discovers that his/her card is missing.

As mentioned earlier, the various customer disputes associated with credit card payments may result in chargebacks. Merchants who cannot resolve such disputes properly or have a high incidence of such chargebacks may lose their ability to provide credit card payment as one of the payment modes to its customers. The merchants may also incur the cost of bank charges and fines imposed by card associations.

3.2.3 Fulfillment

Fulfillment looks at the delivery of goods that are purchased via e-commerce. These could be the delivery of goods ordered via B2B or B2C sites. There are basically 2 modes of fulfillment, i.e. physical delivery of physical goods, and digital delivery of goods.

- **Risk of delivering physical goods**

Physical delivery of physical goods refers to the delivery of tangible products via air, land or sea transportation. The risk involved in physical goods fulfillment is merchantability. Merchantability refers to several scenarios including defective goods or goods not as described, goods not matching description, goods not fit for purpose of purchase and delivery delay.

- **Risk of delivering digital goods**

Digital delivery of goods involves the exchange of digital information over

an intranet, extranet or the Internet. As information is sent through electronic means, it is vulnerable to certain risks such as hijacking and illegitimate manipulation of information content or mass duplication of copyrighted content.

Additionally, if the merchant engages a third party agent to deliver the merchandise and/or collect payment from the customer, the merchant also runs the risk of losing both the merchandise and monies.

3.2.4 Legal & Regulatory Issues

As e-commerce facilitates international transactions, merchants have to be mindful of the implications of overseas laws, taxes and regulations. Businesses should take prudent steps in finding out the appropriate laws and regulatory requirements of the goods and services they intend to sell, especially that of the targeted countries.

4.0 Preventive Measures to Minimise Risks

4.1 HOW TO MINIMISE SECURITY RISKS?

In order for e-commerce to take flight, it is essential to foster trust and confidence between both the merchants and consumers. Confidence can be instilled if they can ascertain the identity of the person they are communicating and/or transacting with, the information and funds exchanged are not been fraudulently tampered with and confidentiality is maintained. In short, merchants and consumers are more willing to embrace e-commerce if a secure e-commerce environment is established in which online transactions and communications can take place. Such an environment can be created through harnessing the various technologies to minimise risks.

4.1.1 Developing a Security and Risk Management Policy

The single most important step to manage a corporate website's security is to create a written security and risk management framework policy. In this document, the organization will analyse and articulate the risks identification, consequences and impact to operations, mitigation and control strategies, and continuous monitoring and review. This policy should succinctly lay out the organisation's website policies with regard to:

- who is allowed to use the system
- when they are allowed to use it
- what they are allowed to do (different groups may be granted different levels of access)
- clear customers' privacy policies
- procedures for granting access to the system
- procedures for revoking access (e.g. when an employee leaves)

- what constitutes acceptable use of the system
- remote and local login methods
- system monitoring procedures
- protocols for responding to suspected security breaches

The security policy serves as a requirements document against which technical solutions can be judged. The promotion of these security policies amongst staff will raise the level of security awareness.

4.1.2 Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is usually used for channel encryption and server authentication. It works by securing the exchange of information between two computers by scrambling the information so it cannot be read by a third party. SSL is a minimum encryption requirement for e-commerce merchants to exchange information with their customers. The current standard is 128 bit.

4.1.3 Firewalls

Firewalls are used to prevent unauthorized access to and from websites. This should also be a basic security requirement for e-commerce merchants. Firewalls can be implemented in the form of hardware or software. The types of firewall and scale of security implemented will depend on the business needs. Merchants must ensure that they configure the firewalls correctly according to their security requirements.

4.1.4 Anti-virus Software

Anti-virus software is used to protect against computer viruses. Anti-virus software should be installed in all computer systems. They should also be

updated regularly to ensure protection against all new viruses that emerged. By taking a proactive stance towards keeping anti-virus software updated can significantly reduce the risk of virus attacks. A majority of the anti-virus software packages in the market come with free regular updates, which merchants can easily download from the Internet. Other measures merchants can take to protect against virus attacks include:

- Taking precautions when opening emails from unknown sources, especially if they contain attachments
- Downloading software from only trusted websites.

4.1.5 Software Patches

A software patch is defined as a temporary fix to a program bug. A patch is an actual piece of object code that is inserted into (patched into) an executable program.

Software companies/ vendors create patches that they post on their website when bugs are discovered in a program that may allow a malicious person to attack the user's computer. Users need to stay informed and be sure to download and install the patches to keep their computer safe.

4.1.6 Network Monitoring

Security risks can affect Merchant's network and systems, from the web servers and e-mail servers to each individual network devices. Having implemented security solutions like firewall does not mean that the network is secure, if there is no monitoring system.

Merchants should have procedures in place to constantly monitor the logs, messages and alarms from all application servers, operating systems, network routers, anti-virus and firewalls. Information available from these logs is very useful when investigating a potential hacker attacks or security breach. Actions can be taken immediately, to reduce further damage.

4.2 HOW TO MINIMISE PAYMENT RISKS?

A lot of payment and transaction information are transmitted via the Internet in online shopping. Most websites utilise common forms of customer authentication for customers such as passwords and Ids. Tools like firewall, anti-virus software, SSL highlighted in the above points help to prevent hackers from stealing card information for fraudulent use on the Internet. Many government agencies and banks use more advanced options such as public key infrastructure (PKI). It is a combination of software and encryption technologies allowing organisations to protect the security of their online communications and transactions. It employs a system known as public key cryptography, together with carefully documented policies, to ensure that transactions are authentic and secure.

Below is a list of precautionary measures that e-commerce merchants can take when handling payment transactions to minimise payment risks:

- All transactions must be authorised online real time. If account funds are available and a card has not been reported lost or stolen, the transaction should be approved by the customer's' bank. .
- E-commerce merchants should note that an authorisation for a credit card is not proof that the true cardholder is making the purchase. Only card scheme approved authentication protocols will guarantee payment to merchants for fully authenticated transactions.
- Due to the absence of face-to-face transactions and verification of cardholder signature in online payments, e-commerce merchants will be exposed to a greater risk of fraudulent or disputed transaction. An e-commerce merchant can be held financially responsible for these transactions, even if the Issuer has approved it. Authentication technologies such as Verified by Visa and SecureCode by MasterCard are currently available in the market and will provide merchants with a guaranteed payment should they attempt to authenticate their cardholders. For more information, you can contact your credit card

processing bank.

- Merchants should ensure that all customer payment data is stored in a secured manner. Unless it is critical to the marketing strategy, merchants are not advised to store account information.
- All merchants should ensure the appropriate data elements are present when submitting Internet transactions for authorisation, for e.g., card payments, it is the Electronic Commerce Indicator (ECI). This allows the Issuer to make a more informed authorisation decision.

4.3 HOW TO MINIMISE FULFILMENT RISKS?

4.3.1 Physical goods

Merchants can invest in technologies that will monitor the purchasing patterns and mailing addresses of customers. Any irregularities tracked will point to possibilities of fraud, to which the merchant can then take the necessary corrective measures. Additionally, merchants who require freight services can establish long-term business relationship with reputable and trustworthy courier agents to minimise incidences of fraud. Merchants can also negotiate with these courier companies to avail tracking facilities so that the delivery of merchandise can be stopped at any time when fraud is discovered.

4.3.2 Digital goods

Through cutting edge technology, the illegitimate replication of digital contents for mass distribution can be done easily, without compromising on the quality of the replicated content. With Digital Rights Management (DRM), content owners can now digitally encrypt their goods to prevent them from being duplicated illegally. The main feature of DRM is its ability to protect information. Any electronic content and intellectual properties such as literary works, graphic and video files, software can also be protected with DRM, both online and offline. It also

Merchants' Guide to Managing e-commerce Risk and Fraud

performs usage tracking of the information, to facilitate the collection of revenues.

5.0 Adopting E-Business Best Practices

Merchants recognise the importance of risk management in order to thrive in e-commerce. However, what is noteworthy is that risk management is not a one-time effort but a continuous process that necessitates organisation-wide involvement. With this in mind, the section attempts to recommend to merchants a set of best practices, which helps address issues such security risks, customer disputes and fraud, all of which are fundamental to the smooth running of an e-commerce business. Merchants can then determine for themselves which are needed in order to maintain a level of security that commensurate with the risk and protection its website requires.

To assist merchants to better manage their e-commerce operations, NTC initiated the TrustSg Programme to encourage adoption of e-business best practices. The main principles of TrustSg can be found in Appendix A. Merchants can also refer to www.trustsg.org.sg for more information on this program and how they can get themselves accredited.

5.1 COMMUNICATION

Merchants should, to its best efforts, communicate all necessary information via its website to customers in a clear, accurate and complete manner so as to reduce customer disputes and dissatisfaction.

5.1.1 Business & General Information

- Provide customers with accurate, clear, conspicuous and concise information that is easily accessible online. At a minimum, merchants should reveal the following information on themselves:
 - name of the business entity as registered with the local authority and name under which it conducts its business (if different from the former);

Merchants' Guide to Managing e-commerce Risk and Fraud

- principal registered/physical address or location where the business entity can be contacted offline;
 - contact number of the business entity that is staffed to receive and respond to enquiries. In the event that the provision of such a number is shown to be disruptive to daily operations, the business entity must maintain a working listed phone number;
 - email address and/or other electronic means that allow prompt and easy communication with the business entity; and
- Develop a "Frequently-Asked-Questions" (FAQ) page that includes questions and answers, which educates customers on how they can protect themselves whilst shopping online.

5.1.2 Product Information

- Disclose all relevant information, in a clear and accurate manner, on the goods and/or services available, sufficient for customers to make an informed transactional decision.
- At a minimum, information presented to the customer should include (where applicable):
 - product descriptions (include product images if possible)
 - prices and customer costs;
 - delivery/shipping information;
 - terms and conditions of the transaction;
 - currencies in international standard; and

- units of measure in international standard.
- Businesses should ensure that when more than one language is made available to customers, all relevant content and information on the transaction must be completely presented in each language.

5.1.3 Confirmation and Payment Information

- Allow customers to review, correct and/or cancel their orders, before confirmation.
- Clearly state, where applicable, all payment mechanisms available for customers to provide payment for goods and/or services. Payment mechanisms for conducting a transaction, where provided, should be secure, reliable and easy-to-use.
- Clearly state how payment information is protected during transmission, while on the merchant's server and at the physical work site.
- Clearly state any terms and conditions and/or policies with regard to change, cancellation or refund of purchases.
- Allow customers to review and confirm their orders before accepting the transaction. At a minimum, the confirmation notification should include information on:
 - itemisation of products and/or services ordered including pricing, delivery, currency, quantity, units of measure and any additional charges;
 - the chosen payment method and terms including the pricing structure, any warranties or fees, relevant taxes or excise duties in relation to goods and/or services offered; and
 - the anticipated date of delivery or performance including the terms of

delivery, any shipping fees or handling fees resulting from a purchase of goods and/or services and the expected timeframe for delivery of the goods and/or services to the customer before the acceptance of an order.

- Highlight to customers that email is not a secure communication method and should never be used to transmit card numbers or other sensitive information

5.1.4 Fulfilment

- Clearly state, where applicable, options available for customers to receive their goods and/or services ordered
- Ensure that, where applicable, the appropriate level of fulfilment and delivery mechanisms, processes and controls are established to comply with representations made to their customers
- Promptly send an email response to customers in the event of a delivery delay

5.2 CUSTOMER DATA MANAGEMENT

Merchants should take adequate steps to protect customers' personal information within their control and management.

- Designate and train an individual or individuals to be accountable for the proper collection, processing and use of customer information
- Take reasonable steps to ensure that personal information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used
- Ensure that personal information is protected by security safeguards appropriate to the sensitivity of the information

The Model Data Protection Code, which sets the minimum standards to collect, manage and process personal data, was officially released by the NTC on 17 Dec 2002. The broad principles of the code can be found in Appendix B. Merchants can also refer to [ww.trustsg.org.sg](http://www.trustsg.org.sg) for a complete set of the Model Data Protection Code.

5.3 SECURITY AND RISK MANAGEMENT

Merchants should develop a comprehensive security and risk management framework, which should be documented and then be communicated to both internal and external users.

- Deploy secure Operating System
 - Operating system software should be properly configured to provide effective security setting consistent with the level of protection required. Software must be kept up-to-date with enhancements, patches and updates installed.
- Set up Firewalls
 - Firewalls must be set up between internal and external networks, and between different geographical sites.
- Use of Intruder Detection Systems
 - Network scanners, intruder detectors and security alerts software are needed to complement firewalls in case of intrusion and unauthorized access.
- Perform Database Backup
 - Regular backup of data should be carried out. However, this should be done with minimal disruption to customers. One way to minimise such

Merchants' Guide to Managing e-commerce Risk and Fraud

disruption is to conduct data backup during low customer traffic. This backup should be stored in a secure manner and ideally offsite. Implement Anti-Virus software and keep the virus signature and pattern files up-to-date

- Install network analyser to assist in analysing the nature of the attack and containing it
- Ensure adequate security logs and audit trails, especially for sensitive files and transactions
- Deploy strong cryptography and key management practices to protect data confidentiality
- Conduct security review of strengths and weaknesses of Internet-based operating system software, application systems and network before each implementation, and regularly thereafter, including penetration testing
- Establish security-monitoring procedures including analyzing security logs for suspicious traffic and access attempts, implementing incident management and response plan
- Provide clear and adequate instructions to customers to ensure they are able to comply with the security functions connected with the operation of the on-line services
- Engage professional security auditors, who possess the requisite skills, to undertake annual audits
- Adopt best practices standards and guidelines for management of ids and passwords, application development controls, high network and system availability, rapid and disaster recovery provision, and security education and awareness programs.

Besides putting in place a good security practice on the computing systems, ensuring physical security of servers/hard wares and internal security is equally crucial.

- Physical security

First, it is important to identify which are the business computers, servers, systems and electronic equipment that are critical to the business operation that require considerable protection from potential physical risk. Next, there is a need to recognise potential physical risks e.g. fire, blackouts, heavy storm / thunderstorm, war / terrorism. Subsequently, corresponding protective measures has to be enforced to make the premise safe to house critical hard wares.

- Fire

- » Train personnel on fire safety
- » High fire rating doors, walls and server racks
- » Use of appropriate fire extinguishers e.g. CO2 fire extinguishers for electronic equipment and computers
- » Fire drills at least once a year

- Blackouts

- » Install un-interrupt power supply (UPS) for critical computer equipment and hardware.
- » Where required, have back up generators. Some buildings may have such facilities.
- » Back up critical business database and systems regularly

Merchants' Guide to Managing e-commerce Risk and Fraud

- Heavy storm/Thunderstorm
 - » If the area of business is prone to flooding, place important servers, computers and other important equipment on higher floors and away from windows. If it is not available, you may place them on high stands.
 - » Install un-interrupt power supply (UPS) for critical computer equipment and hardware
- War / Terrorism
 - » Centralise and tighten access to public areas to the company premise e.g. car parks, loading/unloading bays, lobby etc. Access by messengers and delivery persons must also be controlled and monitored.
 - » Station uniformed security guards at access points and that they are highly visible. Regular patrol should be carried out.
 - » Close circuit television around and inside the business premise.
 - » Regulate visitors to your business premise and have access controls, e.g. register visits by guest and issue visitors pass, prior appointments etc.

- Internal Security

Employees, consultants, vendors and other individuals who have (or had) access to the company's facility, systems and sensitive data (be it digital or otherwise) may perpetrate internal attacks. Such risks are more common than external risks. The reasons for internal attacks may be for monetary gains, revenge (e.g. disgruntled employee) or attention seeking. Therefore, there must be a balance between security and trust. The following may be

considered to mitigate such risk:

- Appointment/Employment

Background checks before hiring employees and vendors especially for those who will require access to the company's critical business systems. For vendors, request for reference sites and visits for the past clients.

- Employee education

Especially on areas about internal theft, mischief, and internal security.

- Develop and implement clear reporting policy and procedures for response to internal attacks.
- Develop and implement strong clearance management policy.
- Develop and implement password/key control policy and procedures

All access codes and PINS to the company main systems should be stored and sealed in an envelope with security seal in a safe. Password files stored in computer system should be strongly encrypted to prevent any illegal access. Where possible, all the passwords and PIN should be changed periodically or on every use or if it deemed compromised.

- Restrict employees' access

Grant access on a need to basis for the employee to carry out his job. Any access to any sensitive facility, document and system should be properly logged and audited.

- Audits

Periodic inspections and audit should be carried out on the storage of sensitive documents, all access logs and reports to the documents and its

destruction.

- Disposal of sensitive documents, data and computer system

Ensure that all sensitive document and data are no longer in use are destroyed thoroughly. For computers, ensure that all sensitive data are removed and have the hard disk reformatted. Although such documents, data and computers are marked for disposal, they should still be accorded with the same security level and treatment as other before its disposal. Auditor and/or the company personnel should be present to ensure and witness that the sensitive document, data and computer are destroyed completely.

5.4 REGULAR MONITORING OF TRANSACTIONS

Merchants should take some simple steps to minimise customer disputes, particularly those arising from card payments, and protect themselves from fraudulent transactions.

- For authorisation-only transactions, an unusual number could indicate testing
- An unusually high quantity, average size or volume of credits could indicate fraud
- Identical transaction amounts
- Transactions without associated customer identification information
- Multiple transactions from a single Internet Protocol (IP) address
- Transactions on similar account numbers
- Multiple transactions on a single card over a very short period of time

Merchants' Guide to Managing e-commerce Risk and Fraud

- Unusual requests
- Unusual timing of transactions
- Unusual electronic message formats
- Anomalies in transaction types
- Anomalies in "log-on violations"
- Be wary of accepting transactions from high risk or third world countries

5.5 REDRESS AND DISPUTE RESOLUTION

Merchants should establish procedures and practices to efficiently and effectively address customer complaints and resolving customer disputes.

- Develop effective in-house procedures for handling complaints; for instance, through customer services or a named individual who is responsible for enquiries/complaints and who has the authority to answer enquiries and resolve complaints
- Clearly state the various levels of redress procedures available to a customer seeking recourse and these procedures should be made easily accessible to the customer

Appendix A

TrustSg Core Principles

1. BUSINESS PRACTICES AND COMMUNICATIONS PRINCIPLE

Businesses engaged in electronic commerce should ensure that fair business, advertising and marketing practices are adopted in their interaction with their customers.

2. DISCLOSURE PRINCIPLE

A Business Entity

Businesses engaged in electronic commerce should provide customers with accurate, clear, conspicuous and concise information, easily accessible online, on themselves.

B Goods and Services

Businesses engaged in electronic commerce should disclose relevant information on the goods and/or services available, sufficient for customers to make an informed transactional decision.

C Confirmation and Payment

Businesses engaged in electronic commerce should allow customers to review, and if necessary, to correct and /or cancel, their orders, before confirming their intent to commit to a transaction. Payment mechanisms for conducting a transaction, where provided, should be secure, reliable and easy-to-use.

D Fulfilment

Businesses engaged in electronic commerce should seek to ensure that they comply with any representations or commitments made to customers on the fulfilment of goods and/or services ordered through electronic commerce.

3. DATA PROTECTION PRINCIPLE¹

Businesses engaged in electronic commerce should take adequate steps to protect customers' personal information² within their control and management.

4. SECURITY PRINCIPLE

Businesses engaged in electronic commerce should formulate and adhere to transparent and clear security measures and policies. The appropriate level of security and protection should be afforded to their customers and their data.

5. AVAILABILITY PRINCIPLE

Businesses engaged in electronic commerce should, where applicable, adopt measures, practices and controls to ensure the appropriate level of reliability and availability of systems, services and data is afforded to customers.

6. REDRESS AND DISPUTE RESOLUTION PRINCIPLE

Businesses engaged in electronic commerce should establish procedures and practices for efficiently and effectively addressing customer complaints and resolving customer disputes arising from its electronic commerce activities.

7. PROTECTION OF MINORS AND THE ELDERLY PRINCIPLE

Businesses engaged in electronic commerce should, where applicable, take into account the level of sophistication and knowledge of minors, the elderly and others that may not have the capacity to fully comprehend information presented to them through the website.

8. ACCESSIBILITY FOR PEOPLE WITH DISABILITIES (optional)

Businesses engaged in electronic commerce are encouraged to make reasonable adjustments where necessary to ensure that the content of their website is accessible to people with disabilities.

¹ The set of guidelines under this principle is based on the Model Data Protection Code for the Private Sector, released by the National Trust Council (NTC).

² Personal information is information about an identifiable individual held in electronic form.

Appendix B

Model Data Protection Code for Private Sector

Principle 1 – Accountability

An organisation is responsible for personal data in its possession or custody.

Where the personal data is under the control of the organisation, the organisation shall, in addition, designate a person or persons who are accountable for the organisation's compliance with the following principles.

Principle 2 – Specifying Purposes

The purposes for which personal data are collected shall be specified by the organisation.

Principle 3 – Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal data to a third party, save where the following exceptions apply:

Collection without knowledge or consent of the individual is permitted where:

- a. All of the following apply:
 - i. the collection is clearly in the interest of the individual;
 - ii. it is impracticable to obtain the consent of the individual to that collection; and
 - iii. if it were practicable to obtain such consent, the individual would be likely to give it.
- b. Collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the data where such collection pertains to an investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being, or is about to be committed;
- c. Data is being collected in an emergency that threatens the life, health or security of a person; or
- d. Collection is of data which is generally available to the public.

Use without knowledge or consent of the individual is permitted where:

- e. All of the following apply:
 - i. the use is clearly in the interest of the individual;
 - ii. it is impracticable to obtain the consent of the individual to that use; and
 - iii. if it were practicable to obtain such consent, the individual would be likely to give it.

Merchants' Guide to Managing e-commerce Risk and Fraud

- f. Data is used in the investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being, or is about to be committed;
- g. Data is being used in an emergency that threatens the life, health or security of a person; or
- h. Use of data which is generally available to the public.

Disclosure to a third party without knowledge or consent of the individual is permitted where:

- i. All of the following apply:
 - i. the disclosure is clearly in the interest of the individual;
 - ii. it is impracticable to obtain the consent of the individual to that disclosure; and
 - iii. if it were practicable to obtain such consent, the individual would be likely to give it.
- j. Disclosure is made to a solicitor representing the organisation;
- k. Disclosure is necessary for the purposes of establishing, exercising or defending legal rights;
- l. Disclosure is to a government agency that has made a lawful request for the data;
- m. Disclosure is made to a person who needs the data because of an emergency that threatens the life, health or security of a person;
- n. Disclosure is made to an institution whose purpose is the conservation of records of historic or archival importance and disclosure is for such purpose;
- o. Disclosure is of data which is generally available to the public in that form; or
- p. Disclosure is reasonable for purposes related to the investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being or is about to be committed.

Principle 4 – Limiting Collection

Except as provided below, the collection of personal data shall be limited to that which is necessary for the purposes specified by the organisation.

Data shall be collected by fair and lawful means.

Collection beyond purposes specified is permitted where:

- a. All of the following apply:
 - i. the collection is clearly in the interest of the individual;
 - ii. it is impracticable to obtain the consent of the individual to that collection; and
 - iii. if it were practicable to obtain such consent, the individual would be likely to give it.
- b. Collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the data where such collection pertains to an investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being, or is about to be committed;
- c. Data is being collected in an emergency that threatens the life, health or security of a person;
- d. Collection is of data which is generally available to the public; or
- e. The individual consents to the collection.

Principle 5 – Limiting Use, Disclosure, and Retention

Except as provided below, personal data shall not be used or disclosed to a third party for purposes other than those for which it was collected, unless the individual consents to such use or disclosure.

Subject to any applicable legal requirements, personal data shall be retained only as long as necessary for the fulfilment of those purposes.

Use beyond the purposes for which it was collected is permitted where:

- a. All of the following apply:
 - i. the use is clearly in the interest of the individual;
 - ii. it is impracticable to obtain the consent of the individual to that use; and
 - iii. if it were practicable to obtain such consent, the individual would be likely to give it.
- b. Data is used in the investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being, or is about to be committed;
- c. Data is being used in an emergency that threatens the life, health or security of a person;
- d. Use of data which is generally available to the public; or
- e. The individual consents to the use.

Disclosure beyond the purposes of collection is permitted where:

- f. All of the following apply
 - i. the disclosure is clearly in the interest of the individual;
 - ii. it is impracticable to obtain the consent of the individual to that use; and
 - iii. if it were practicable to obtain such consent, the individual would be likely to give it.
- g. Disclosure is made to a solicitor representing the organisation;
- h. Disclosure is necessary for the purposes of establishing, exercising or defending legal rights;
- i. Disclosure is to a government agency that has made a lawful request for the data;
- j. Disclosure is made, on the initiative of the organisation, to an investigative body appointed by the organisation, or to a government agency for investigative purposes;
- k. Disclosure is made to a person who needs the data because of an emergency that threatens the life, health or security of a person;
- l. Disclosure is made to an institution whose purpose is the conservation of records of historic or archival importance and disclosure is for such purpose;
- m. Disclosure is of data which is generally available to the public in that form; or
- n. Disclosure is made by an investigative body and the disclosure is reasonable for purposes related to the investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being or is about to be committed.

Principle 6 – Accuracy

Personal data shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

Principle 7 – Safeguards

Personal data shall be protected by appropriate security safeguards.

Principle 8 – Openness

An organisation shall make readily available information about its policies and procedures for handling personal data.

Principle 9 – Individual Access and Correction

Subject to the following exceptions, an individual shall upon his request be informed of the existence, use, and disclosure of his personal data and shall be given access to that data. An individual shall be able to challenge the accuracy and completeness of his personal data and have them amended as appropriate. The reasons for denying access should be provided to the individual upon request.

The organisation shall refuse the request where:

- a. Providing access would be likely to reveal personal data about another person, unless
 - the said person consents to the access; or
 - the individual needs the information because a person's life, health or security is threatened,provided that where the data about the said person is severable from the record containing the data about the individual, the organisation shall sever the data about the said person and shall provide the individual access; or
- b. An investigative body or government agency, upon notice being given to it of the individual's request, objects to the organisation's complying with the request in respect of its disclosures made to or by that investigative body or government agency;

The organisation may refuse the request where:

- c. Data is protected by solicitor-client privilege;
- d. It would reveal data that cannot be disclosed for public policy, legal, security, or commercial proprietary reasons,
- e. Provided that where the personal data about the individual is severable from the record that cannot be disclosed for public policy, legal, security or commercial proprietary reasons, the organisation shall sever the data and give the individual access;
- f. It would threaten the life, health or security of a person;
- g. Data was collected under 4.3(b) (generally, collection pertaining to an investigation of

- a breach of an agreement or the law);
- h. Complying with the request would be prohibitively costly to the organisation; or
- i. The request is frivolous or vexatious.

Principle 10 – Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated person or persons accountable for the organisation's compliance.

Glossary

Acquirer

A financial institution that enters into a contractual relationship with a merchant for purposes of accepting payment cards.

Audit Trails

A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. Sometimes specifically referred to as a security audit trail.

Authentication

The process by which the identity of a user logging onto a computer system is verified or the integrity of a transmitted message is verified.

Cryptography

The mathematical process of protecting information by transforming it into an unreadable format so that it can be safely transmitted over a public network such as the Internet. The information is then decrypted later when it is used again.

Encryption

A way of coding information in a file or e-mail message so that if it is intercepted by a third party as it travels over a network it cannot be read.

Internet

A network of computers that share the same protocol called the TCP/IP. Each computer runs software that provides or "serves" information to another computer. The Internet is

Merchants' Guide to Managing e-commerce Risk and Fraud

the transport vehicle for information that is stored in files or documents on another computer. It is sometimes compared to a giant international plumbing system. The Internet itself does not contain information.

Internet Protocol Address

A unique numerical address that is assigned to each computer connected to the Internet.

Issuer

A financial institution that enters into a contractual relationship with a cardholder for issuance of one or more payment cards.

Log-on Violations

When password is required to gain access to a system, any erroneous attempt will be registered as login violations.

Network Analyser

A network is a group of computers set up to communicate with one another. A network can be a small system that's physically connected by cables (a LAN), or you can connect separate networks together to form larger networks (called WANs). The Internet, for example, is made up of thousands of individual networks. As such, a network analyser is the one who oversee and administer the operation of the network.

Operating System

Software that supervises and controls tasks on a computer.

Password

A word or code that is entered into the system to access data. It protects against any unauthorised access.

Security Log file

A file that record all events or activities related to security that have taken place on a computer.

Secure Socket Layer (SSL)

SSL is the industry-standard method for protecting web communications. It provides data encryption, server authentication, message integrity and optional client authentication.

Reference list

Local Reference Portals

Business.gov.sg http://www.business.gov.sg/bizTopic/eCom/eCom_main.htm

Ministry of Law <http://www.gov.sg/minlaw/hq/abt.html>

Electronic Commerce Singapore <http://www.ec.gov.sg>

Intellectual Property Office of Singapore <http://www.ipos.gov.sg/about/message.html>

Inforcomm Development Authority of Singapore <http://www.ida.gov.sg>

Singapore Broadcasting Authority http://www.sba.gov.sg/sba/i_codenpractice.jsp

Guideline / Best practices

TrustSg <http://www.trustsg.org.sg>

VISA <http://www.visa-asia.com/verified/merchants.shtml>

MasterCard <http://www.mastercard.com/sg/merchantcenter/ecom.html>

CitiBank <http://www.citibank.com.sg>

CommerceTrust Ltd <http://www.commercetrust.com.sg>

PKI forum Singapore <http://www.pkiforumsingapore.org>

System Security

TrustMarque International	http://www.trustmarque.com
Integral Solutions Asia (Pte) Ltd	http://www.datamining.com.sg
Trend Micro	http://www.antivirus.com
Mcafee.com	http://www.mcafee.com