

MERCHANTS' GUIDE ON MANAGING E-COMMERCE RISK AND FRAUD – FAQ FORMAT

E-commerce offers competitive advantages such as improved productivity, reduced costs, streamlined business processes, improved customer service and entry to the global business arena. Online shopping is still growing although credit card security and online fraud remain the biggest concerns of online retailers. Online retailers have found that online fraud has adversely affected their bottom lines. According to consulting company Gartner, international losses from online fraud, particularly among the largest online retailers, amounted to US\$1.64 billion in 2002 from a total of US\$91 billion in online sales revenues¹. This is twice the amount of US\$700 million in 2001 from US\$61.8 billion in online sales revenues

What is the Risk & Fraud Management Framework? Why was it developed?

Operating an online business involves risks and challenges, but if merchants are aware of the risks and observe best business practices to address these risks, they will be better able to reap the benefits from e-commerce. The National Trust Council (NTC) has thus developed the “E-commerce Risk and Fraud Management Framework” to educate B2C merchants on the potential risks associated with operating online businesses as well as best practices to address these risks.

B2C merchants who will benefit from this framework include:

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

What does the framework tell me?

The framework contains comprehensive information on the benefits of conducting e-commerce operations, types of e-commerce risks and their implications, preventive measures to minimise risks and e-commerce best practices. The full document can be downloaded from www.trustsg.org.sg.

What are the common issues and concerns in operating online businesses?

Some of the common issues and concerns for merchants with regard to operating online businesses include the need to differentiate legitimate customers from fraudulent users in real time, establish 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.

What are some of the potential risks I will face when setting up an e-business?

The potential risks that you would face are namely security, payment and fulfillment risks.

¹ “Card networks promise higher online shopping traffic”, The Asian Banker, 6 February 2003

Security risk

Security risk arises from virus and hacker attacks. The severity of the damage caused varies with the type of attack (e.g. data loss, stolen information, denial of service, etc.). Viruses and hacker attacks disrupt your business operations and can lead to loss in customer confidence and sales revenue.

Payment risk

Payment risk exists when transactions are done over the Internet and when the customer's identity could not be identified/established. This gives rise to payment disputes from genuine customers. Such situations are more commonly associated with credit card payments over the Internet. Other reasons for payment disputes can arise from ordered goods not reaching the customer, disagreement over the currency conversion rate, goods received are not according to the customer's specification.

Fulfillment risk

Fulfillment refers to the delivery of goods, which could be physical/ tangible products or digital goods. Fulfillment risks associated with physical goods refer to scenarios such as defective goods, goods not matching description, and delays in delivery. Digital goods fulfillment is performed via electronic means and is vulnerable to risks such as hijacking and illegitimate manipulation of information content or mass duplication of copyrighted content.

What can I do to minimise these risks?

The framework outlines the various methods or steps businesses can take to minimise these risks. It recommends that businesses should adopt a disciplined approach in risk management and bear in mind that risk management is not a one-time effort. It is a continuous process that requires organisation-wide commitment and well-documented procedures, processes and practices to manage security, payment and fulfillment risks. For example, you can develop a security and risk management policy, which identifies and analyses risks, and the potential impact that they will have to your operations. This policy should be promoted widely amongst staff to raise the level of awareness. You can also invest in various technologies to authenticate customers' identities to minimise payment risks, and technologies to monitor purchasing patterns to reduce fulfillment risks.

About the National Trust Council (NTC)

The National Trust Council 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 is the nationwide trust mark programme – TrustSg. TrustSg is an approved accreditation scheme that recognises, accredits and promotes 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. In addition to the “**E-Commerce Risk and Fraud Management 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.

For more information on the TrustSg Programme, please contact the TrustSg Secretariat at:

Phone: +65 6211 1752
Fax: +65 6211 2234
Email: admin@trustsg.org.sg
URL: www.trustsg.org.sg