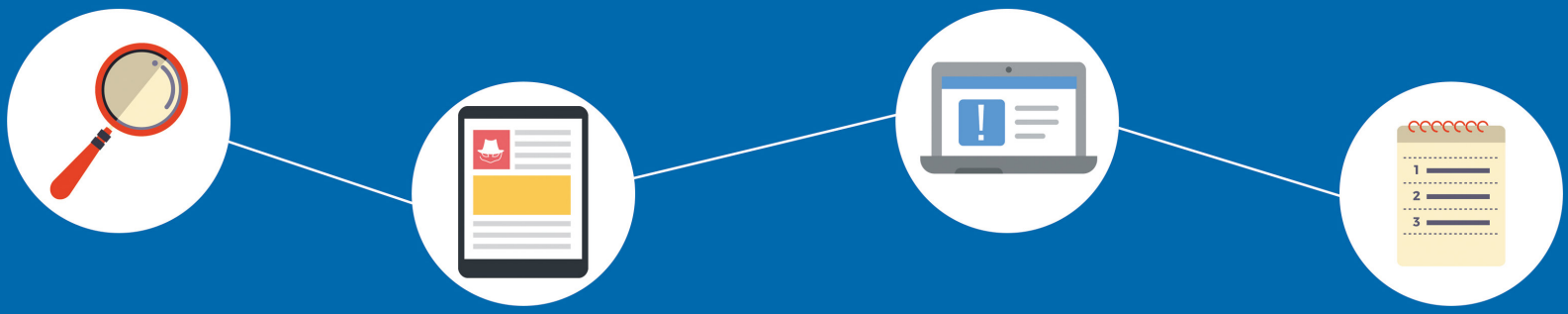
15 Steps to Managing E-commerce Risk



The following steps have been identified as those that are most important to managing e-commerce risk.

E-COMMERCE START-UP

1. Know the risks and train your staff	Your exposure to e-commerce risk depends on your business policies, operational practices, fraud prevention and detection tools, security controls, and the type of goods or services you provide. Your entire organization should have a thorough understanding of the risks associated with any Internet transaction and should be well-versed in your unique risk management approach.
2. Select the right acquirer/ payment processor and service provider(s)	If you have not yet launched an electronic storefront, you need to partner with a Visa acquirer or payment processor that can provide effective risk management support and demonstrate a thorough understanding of Internet fraud risk and liability. You also want to take a good, hard look at any service provider before you sign a contract. Bottom line? Does the service provider have what it takes to keep your cardholder data safe and minimize fraud losses?

WEBSITE UTILITY

3. Develop essential website content	When designing your website, keep operational needs and risk factors foremost in your mind. Key areas to consider are privacy, reliability, refund policies, and customer service access.
4. Focus on risk reduction	Your sales order function can help you efficiently and securely address a number of risk concerns. You can capture essential Visa card and cardholder details by highlighting required transaction data fields and verifying the Visa card and customer data that you receive through the Internet.

FRAUD PREVENTION

5. Build internal fraud prevention	By understanding the purchasing habits of your website visitors, you can protect your business from high-risk transactions. The profitability of your virtual storefront depends on the internal strategies and controls you use to minimize fraud. To avoid losses, you need to build a risk management infrastructure, robust internal fraud avoidance files, and intelligent transaction controls.
6. Use Visa tools	To reduce your exposure to e-commerce risk, you need to select and use the right combination of fraud prevention tools. Today, there are- a number of options available to help you differentiate between a good customer and an online thief. Key Visa tools include Address Verification Service (AVS)*, Card Verification Value 2 (CVV2)**, and Verified by Visa.

CONTINUED ON THE NEXT PAGE

TRANSNATIONAL™
PAYMENTS • TECHNOLOGY • TRUST

FRAUD PREVENTION CONT.

7. Apply fraud screening	Fraud-screening methods can help you minimize fraud for large-purchase amounts and for high-risk transactions. By screening online Visa card transactions carefully, you can avoid fraud activity before it results in a loss for your business.
8. Implement Verified by Visa	The tool Verified by Visa can create the most significant reduction in merchant risk exposure by increasing transaction security through cardholder authentication and by providing chargeback protection against fraud. E-commerce merchants who work with their acquirers to implement Verified by Visa are protected from certain fraud-related chargebacks on all Consumer and Commercial cards with limited exceptions. If applicable, E-commerce merchants may receive a reduced interchange rate.
9. Protect your merchant account from intrusion	Using sophisticated computers and high-tech smarts, criminals are gaining access to shopping cart and payment gateway processor systems, attacking vulnerable e-commerce merchant accounts, and making fraudulent merchant deposits. By taking proactive measures, you can effectively minimize this kind of cyber attack and its associated fraud risks.

VISA CARD ACCEPTANCE

10. Create a secure process for routing authorizations	Before you accept Visa cards for online payment, you must ensure that you have a secure and efficient process in place to submit authorization requests through the Internet.
11. Be prepared to handle transactions post-authorization	There are a number of steps you can take to deal effectively with approved and declined authorizations before you fulfill an order. The idea here is to apply appropriate actions that best serve your business and the customer.

CARD HOLDER INFORMATION SECURITY PROGRAM

12. Safeguard cardholder data through PCI DSS compliance	The Payment Card Industry (PCI) Data Security Standard (DSS) provides e-commerce merchants with standards, procedures, and tools for data protection. For maximum security, you need reliable encryption capabilities for transaction data transmissions, effective internal controls to safeguard stored card and cardholder information, and a rigorous review of your security measures on a regular basis. PCI DSS compliance can help you protect the integrity of your operations and earn the trust of your customers.

CHARGEBACK AND LOSS RECOVERY

13. Avoid unnecessary chargebacks and processing costs	For your business, a chargeback translates into extra processing time and cost, a narrower profit margin for the sale, and possibly a loss of revenue. It is important to carefully track and manage the chargebacks that you receive, take steps to avoid future chargebacks, and know your representment rights.
14. Use collection efforts to recover losses	You can often recover unwarranted chargeback losses through a well-thought through collections system.
15. Monitor chargebacks	Merchants with chargeback monitoring mechanisms are in a better position to spot excessive chargeback activity, identify the causes, and proactively bring chargeback rates down by applying appropriate remedial actions.