Preventing E-Commerce Fraud

Conducting business online presents countless opportunities to enhance customer relationships, attract new business and increase revenue. However, without the security of a physical credit card and signature verification, cyber thieves have an advantage and opportunities for fraud. It is up to the e-commerce merchant to apply the right tools and controls to verify cardholder identity and the validity of transactions. With these controls, merchants can reduce fraudulent transactions and the risk of customer disputes.

Take these steps to effectively manage e-commerce risk:

1. **Evaluate risks and train accordingly.** Examine your business, and determine your unique set of risks. Risks might include fraud, account information theft or chargebacks, depending on the type of goods or services you provide and your specific business policies. Ensure your employees understand these risks and how to mitigate them.
2. **Select the right payment processor.** Ask service providers what steps they take to manage the risk of fraud before signing a contract. Bank and payment processing providers should provide risk management support and have a comprehensive understanding of e-commerce fraud risk and liability concerns.
3. **Design your website with operational needs and risk factors in mind.** To avoid customer misunderstandings and eventual disputes, make your privacy, shipping, return and refund policies accessible on your site, and aim for easy and simple navigation. Communicate your security controls clearly.
4. **Focus on risk reduction.** Establish your sales order process to address risk concerns. Highlight required transaction fields, verify card and cardholder data, use cookies to recognise customers and identify high-risk international addresses.
5. **Design and implement internal fraud prevention structure.** Internal strategies and controls like maintaining an internal database of fraudulent transactions and setting goals for reducing fraud as a percentage of sales can promote profitability.
6. **Make use of fraud prevention tools.** Widely used tools include Address Verification Service (AVS), Card Security Verification Codes, Verified by Visa® and MasterCard® SecureCode.
7. **Implement fraud screening procedures.** Screen online card transactions to minimise fraud for large-ticket items and high-risk transactions.
8. **Protect your merchant account from intrusion.** Minimise the risk of cyber thieves gaining access to your account or payment gateway and making fraudulent fund deposits through the use of monitoring, passwords and information security efforts.
9. **Create a secure process for routeing authorisations.** Set up a secure process for submitting authorisation requests online before accepting card payments over the internet.
10. **Prepare to handle transactions post-authorisation.** Evaluate how you will deal with approved and declined authorisations before fulfilling an order. Require e-mail order confirmations for approved transactions, and review declined authorisations to take appropriate actions.
11. **Reduce chargebacks.** Chargebacks are costly in several ways, increasing processing time, hurting profits and affecting revenue. Tracking and managing chargebacks will help you take steps to prevent them. Act promptly when they happen.
12. **Use collection efforts to recover losses.** Compensate for unwarranted chargeback losses through an effective collections system. Often contacting the customer directly produces results. Outsource remaining customers to a collections agency.

Crendon
Insurance
Brokers

www.crendoninsurance.co.uk
enquiries@crendoninsurance.co.uk

11 Greenfield Crescent, Edgbaston, Birmingham B15 3AU
Tel: 0121 45 45 100