SAFE SALES, SAFE REVENUE

Public awareness and prevention

Taking your business online to the e-commerce world is a big step. We can help you sell securely. Here are some questions and answers to get you started.

Safe sales revenue infographic - Advice for e-commerce businesses

Safe sales, safe revenue poster

PREPARE FOR BUSINESS

WHERE SHOULD I START?

- Know your product

  Some products are riskier to sell than others. For example, selling easily resalable small items that are already in demand is riskier than personally designed items.
- Know your customer

  If you accept card payments and ship valuable goods to your customers, you'd want to know who you are sending the items to, wouldn't you?
- Establish a safe means of payment

  Your card processor can advise you. Choosing a safe means of payment will limit the risk of fraud.
- Use a reliable delivery service

  Choose a delivery method where you can be sure of the professional handling of your merchandise and possible non-delivery dispute claims.

HOW CAN I SELL ONLINE?

To sell goods or services online, you need to have an arrangement with an acquiring processor (also known as an acquirer, payment gateway, card processor, payment processor, etc.). You can think of it as the partner (it could be a bank, but there are other options as well) that receives the electronic payment from your customers and further transfers the money to you.

There are numerous options available. Choose the most suited to your needs and budget. Talk to other retailers about their experience. You can also search the internet for 'acquiring processor in your country', and you will likely find the options available near you.

AS A BUSINESS OWNER THIS IS ALL NEW TO ME. WHAT QUESTIONS SHOULD I ASK THE ACQUIRING PROCESSOR?

- What fraud and risk processes do you offer as standard and which are classed as additional services?
- What chargeback* reports will you provide and how frequently?
- What assistance do you provide your merchants to represent chargebacks?
- What is your overall fraud rate as an acquirer?
- What do you consider an expected fraud rate for a merchant in our category?

* A chargeback is a dispute originating with a genuine cardholder or their card-issuing bank. There are hundreds of reasons why a chargeback may be raised. The card issuer will send details via the related card scheme (Visa, MasterCard, Amex, etc.) to your acquirer who will in turn send you the details. A typical chargeback is when a cardholder sees a sale on their statement that they don't recognise and they dispute it via their card issuing bank. You have options to represent the charge if you have proof the customer was genuine.

HOW DO I CHOOSE AN E-COMMERCE PLATFORM?

Engage your acquiring processor as early as possible. When considering how to sell your goods or services online you can choose to build your own online store or use an existing marketplace.

Research the most trusted marketplaces and pay attention to the services and security measures they include, as well as the fees they charge.

If you prefer creating your own website instead, you can configure a modular webshop system yourself or you can hire the services of a professional company to develop and design the website.

SET UP YOUR DEFENCES

What can I do to protect my e-shop from cybercrime?

It is important to talk to your acquiring processor for advice and website provider for support. They can explain the risks of cybercrime, as well as the solutions fo detection and prevention. Common cybersecurity steps include regularly patching up your software, using strong passwords and installing a firewall and antivirus software. It is important that your webshop is updated regularly, because older versions carry security weaknesses that are patched in later versions. Also remember to change your passwords regularly and follow a password standard that is not easy to break (for example using your shop name as your password is not a good idea).

If possible, use a professional IT service provider to maintain your website security. This can help ensure your company, online store and customer data are kept as secure as possible.

In addition, your acquiring processor will have tools available to help you verify your customer or provide risk scoring relating to customers purchasing from your store. If you want to use additional security, these types of services are also offered by third parties.

They are called 'scoring services' because they provide you with a numerical value of how risky the purchase event is based on their analysis, ranging from 1 (very safe) to 10 (very risky). They check things such as the validity of the card details, if the customer has been on your website before, if the customer is a person or a bot, etc. For example, a reason to lower the score may be that the delivery address is a hotel lobby, not an existing residential address.

If you have employees, make sure they are cybersecurity aware. Encourage them to adopt safe security habits to protect the company and consumer data. You can find some materials that you can use to educate your employees here: mobile malware, cyber scams, CEO fraud.

What do I do if my e-commerce site/online store is attacked?

In the event that your site is hacked, work with your website provider to recover lost data. Engage a dedicated IT support company if possible.

Make sure you have an incident management plan in place. Ensure that your site and data are regularly backed up to a safe, offsite server or service, so you can restore them (for instance, in the event of a ransomware attack).

If there is a ransomware attack, visit No More Ransom for more details.

In case of any type of attack, always gather all possible information and report it to your national police.

As a merchant I need to protect my business against fraud. What does this mean?

Fraud is any wrongful or criminal deception intended to result in financial or personal gain for the fraudster. There are many ways a criminal can target your business, e.g. hacking your customer data, hacking your website, pretending to be a genuine customer but using stolen credentials and payment methods such as stolen payment card details, etc.

Fraud can affect your business in many ways not limited to:

- loss of revenue;
- chargebacks/cardholder disputes;
- reputational damage;
- fines/penalties for non-compliance with retail industry standards and regulations relating to fraud prevention and data security.

Talk to your acquiring processor to ensure your business is protected and compliant with all the relevant fraud prevention payments standards and regulations. They will provide you with more details on the fraud types that affect retailers and the solutions you should put into place for prevention.

What measures should I take to secure my business against fraud?

Ensuring all your employees are aware of the fraud issues affecting online stores is the first step towards fraud prevention. Ensure you stay up to date on the types of payment fraud affecting businesses and you have the tools in place to prevent them. Your national payments organisation will have details on payment fraud types. Your acquiring processor can provide more details about

- PCI DSS (the Payment Card Industry Data Security Standards), to ensure your online payment processing system is secure and your business is PCI compliant;

- How to manage customer activity to decide if a customer is genuine or not;
- Available fraud prevention tools. They are numerous and the more you use, the safer your business will be. Online, just as offline, the cost of implementing good security methods can be high; however, often the financial losses caused by fraud far outweigh the benefits of spending on fraud prevention methods and solutions. Think of it this way: if you had a physical shop, you would likely invest in putting a strong lock on the front door, as well as a padlock, an alarm system, cameras and so on, with each element offering a greater level of security. Just do the same thing online;

Types of fraud solutions available include (the list is not exhaustive):

- CVN – Cardholder verification number (also known as CVV, or Card Security Code
- The three digits on the back of a credit card, or four digits on a charge card)
- AVS – Address verification system
- Telephone number verification/ reverse lookup
- Social networking site checks – find your customers on social media
- Google map look-ups – verify if their address is genuine

- Email address validation
- Postal address validation services
- Payer authentication (3D Secure)
- Paid-for public record services
- Credit history check
- 2-Factor authentication
- Biometric indicators (e.g. voice recognition)
- Negative lists (in-house lists)
- Customer order history

- Order velocity monitoring
- Fraud scoring model (company specific)
- Positive lists
- Customer website visitor behaviour analysis
- Shared negative lists – shared hotlists
- Multi-merchant purchase velocity/ identity
- IP geolocation information
- Device fingerprinting

What are some of the most common types of e-commerce fraud?

- Clean fraud – where the customer has sufficient information to verify they are a 'genuine' customer, but the sale turns out to be fraudulent.
- Phishing – where a criminal will send emails purporting to be from you to dupe customers into sharing their financial details.
- Spoofing – when a criminal creates a website to appear as if it is yours, to take payments from unsuspecting consumers.
- Money laundering – a criminal might purchase high-value goods from your store, then return them and ask that you refund to a different payment source, e.g. the original sale could be on a stolen payment card and the refund to an account owned by the criminal.
- Account take over – where a criminal has taken over a genuine customer's account.
- Discount/refund abuse – where a criminal will use stolen discount codes to buy items at a lower price which they then sell at a higher price elsewhere.

More details on retail fraud types are available at the Merchant Risk Council website .

SELL AND GET PAID SAFELY

HOW CAN MY CUSTOMERS PAY?

- The payment methods you decide to accept could be specific to the country in which you are doing business. Each payment method will have a different cost for you. Discuss all the options with your acquiring processor, who can explain the requirements needed to verify that your customers are genuine and to enable them to pay securely. A basic principle is that your regular customers are less of a risk to your business and as such, you can offer them more payment options.

HOW CAN I VERIFY MY CUSTOMERS' PAYMENT?

The unique payment cards Chip and PIN, were introduced to stop lost/stolen fraud and counterfeit fraud in stores. Similarly, 3D Secure (MasterCard SecureCode and Verified By Visa) was introduced to prevent fraud online.

Talk to your acquiring processor about 3D Secure and how to ensure you have the most up to date version. 3D Secure enables you to verify the customers through several factors of authentication, which they need to provide during the purchase. Under the Payments Services Directive (PSD2) you are required to use the latest version of 3D Secure on your website when selling online to cardholders.

There are options available for you to require the consumer to verify things such as the device they are using, a PIN, password or a passcode that is sent to their phone, their address, specific pre-defined security answers, etc. Your acquirer will guide you on the tools and options available to help you verify your genuine customers.

HOW CAN I ENSURE THE SAFE DELIVERY OF MY GOODS?

Start by talking to your acquiring processor. They will have advice on how to safely deliver goods to your customers.

- Work closely with your chosen delivery/ logistics company. Use reputable brands, with a strong industry presence and a wealth of experience.
- Stay up to date with the criminal activities affecting similar businesses.
- Ensure your delivery firm delivers to the address on the package. Allow rerouting only for well-known customers and determine which items can be rerouted and which ones cannot.
- Verify the customer's address in advance and ensure the delivery company also verifies they delivered to the correct address and addressee.
- Consider enabling delivery and signature confirmation to prove the order was delivered to the intended recipient

WHAT DO I NEED TO KNOW ABOUT CUSTOMER DATA PROTECTION?

When processing customer data such as payment card details, you are required to be PCI Compliant (see above). Meeting the card security standards ensures you are keeping your customer data secure. Talk to your acquirer about how you can ensure compliance.

You will have heard of the General Data Protection Regulation (GDPR). Under the EU Regulation, you are required to explicitly ask your customers for consent to hold any personal data.

WHERE CAN I FIND OUT MORE?

The Payments Association in each country will have details on retail fraud.

Other resources available where you can find more information:

- European Central Bank Fraud Report (PDF)
- Fraud Smart
- Merchant Risk Council - RapidEdu Training Courses on all things fraud, payments and risk for e-commerce retailers

Turn to expert companies when it comes to insurance and risk mitigation.

If you come across any illegal activity, get in touch with your national police.

TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other

---

Source URL: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/safe-sales-safe-revenue