WELCOME TO E-COMMERCE WITH SECUREPAY ONLINE PAYMENTS

Best practice in e-commerce and online payment security

WELCOME TO SECUREPAY

Congratulations! Your SecurePay Online Payments application has been approved and you're one step closer to launching your own e-commerce business.

This welcome kit and e-commerce compliance guide will help you to get a thorough understanding of the compliance process and the benefits and responsibilities that come with SecurePay Online Payments.

We have also provided some best-practice information on how to avoid credit card fraud and protect customer payment card data.

We wish you the best of luck with your e-commerce business and look forward to helping you grow!

MY APPLICATION IS COMPLETE – WHAT HAPPENS NOW?

SecurePay has set up your payment gateway and your internet merchant account – the two essential elements your business needs to be able to sell online. You have received your test and live account credentials via email, so you or your website developer can integrate SecurePay Online Payments into your e-commerce site and test the functionality, ready to go live.

However, before you can start using your new online payments solution, we will need to find out some more information about you and your business. This is a standard process for all businesses in Australia that want to accept online payments.

BEFORE YOU GO LIVE …

The first time you log in to your live SecurePay Online Payments account, a compliance form will be displayed. You are required to fill this in before you can start selling online. The questions in the form cover the standard elements that any e-commerce website in Australia must include.

Once you have completed and submitted your compliance form, your SecurePay Online Payments account is ready, and you or your web developer can launch payments on your website.

WHAT IF I CAN'T COMPLETE ALL THE QUESTIONS?

If you are not able to fill in every field in the compliance form, you will need to make changes to your e-commerce website to ensure you have all the compulsory elements required.

For instance, if your site does not have a terms and conditions page and you weren't able to provide a link to that for the compliance form, you or your web developer will need to go back and add terms and conditions to your website.

Once this is updated, log back in to your live SecurePay Online Payments account and complete the compliance form. Once you have filled in all the fields, you will be ready to go live and start selling online. You can call 1300 656 372 (option 1) if you have any queries.

WHAT WILL SECUREPAY BE CHECKING?

In order to complete the compliance form, you'll be asked to confirm that the following details are present on your website:

- **Contact details**
- **Pricing**
- **Refund policy**
- **Privacy policy**
- **Terms and conditions**
- **Security policy.**

SIX REQUIREMENTS FOR YOUR WEBSITE

1 CONTACT DETAILS
Should include the ABN, a postal address, physical address, email address (if possible) and phone number.

2 PRICING
The currency and the actual price of each item on a website must be clearly displayed.

3 REFUND POLICY
How customers can return or cancel an order and request a refund.

6 SECURITY POLICY
Should describe the security measures in place to protect customer communications, details and payments (for example, SSL certificates and SecurePay).

4 PRIVACY POLICY
Must state how customer details are protected, who a business might share details with in order to do business (for instance, you may need to share details with your delivery supplier) and how customers can get access to their personal data.

5 TERMS AND CONDITIONS
Outlines the legal terms governing the use of the website.

WHAT YOUR PRIVACY POLICY COVERS

Australian businesses must tell customers what they're doing with the personal information they collect during a transaction. This statement could cover:

- What customer data is collected and tracked (including if you use cookies, for instance)
- What the information will be used for (be specific and let customers know if it will be used for marketing purposes)
- Who information is shared with (name the types of third parties – e.g. delivery services – that will receive some customer information)
- How you keep data secure (e.g. internal privacy policies, access to customer information, etc)
- The process if customers want to access or correct their information (provide a contact email address or telephone number).

A web search for "website policy templates for Australia" will provide tools and examples, or visit the website of the Federal Privacy Commissioner: privacy.gov.au.

WHAT YOUR REFUND POLICY COVERS

Your refund and exchange policy must be clear and comply with Australian Consumer Law (ACL). To satisfy the consumer guarantees provisions of the ACL, businesses that supply defective goods must provide repairs, a replacement or a refund. If there is a major failure with a purchase, the customer may choose the remedy they prefer, including requesting a refund.

Goods and services bought online must meet the same statutory conditions and warranties as for in-store sales. Consumers' statutory rights are also the same.

REFUND POLICY EXAMPLE

The Australian Competition and Consumer Commission (ACCC) provides the following principles for a refund policy:

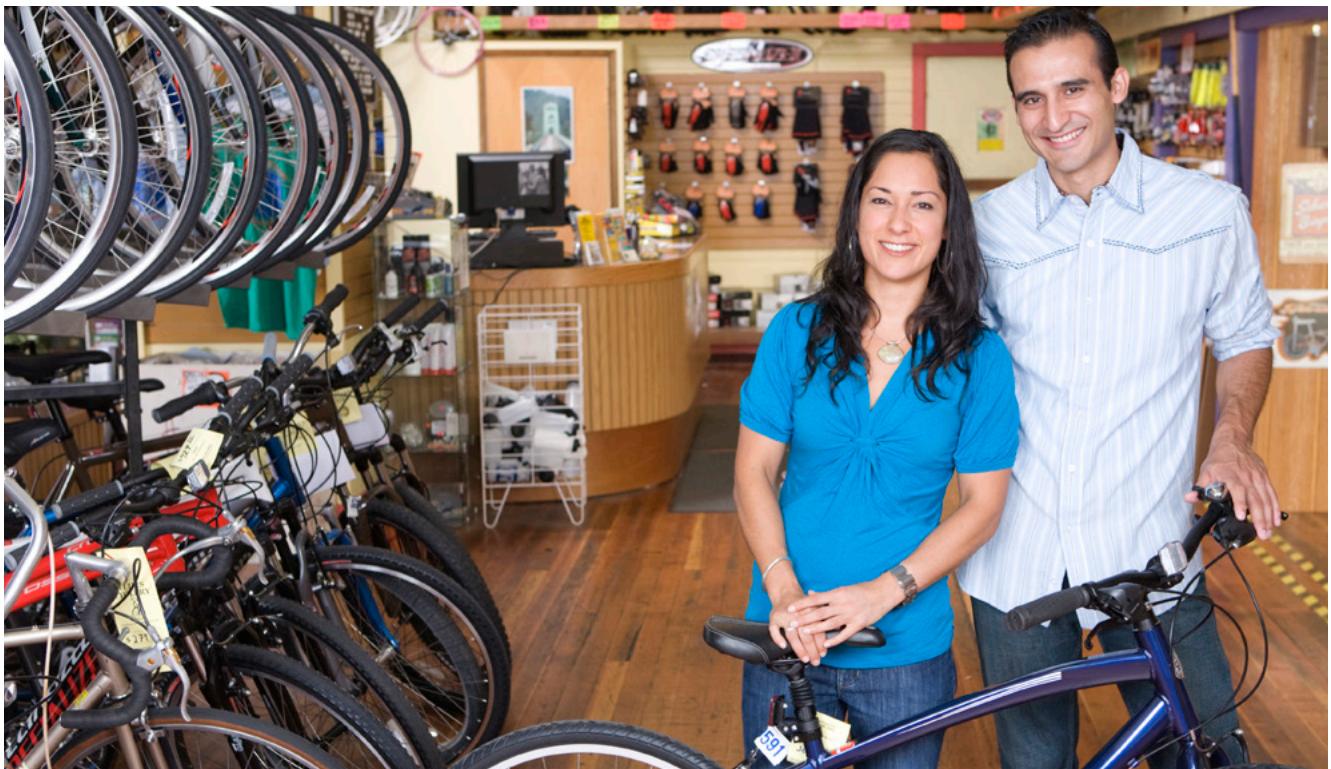
"We are not required to provide a refund or replacement if you change your mind.

But you can choose a refund or exchange if an item has a major problem. This is when the item:

- Has a problem that would have stopped someone from buying the item if they had known about it
- Is unsafe
- Is significantly different from the sample or description, or
- Doesn't do what we said it would or what you asked for and can't be easily fixed.

Alternatively, you can choose to keep the item and we will compensate you for any drop in value. If the problem is not major, we will repair the item within a reasonable time. If it is not repaired in a reasonable time, you can choose a refund or replacement.

Please keep your proof of purchase – for example, your receipt."



MAKING E-COMMERCE SAFER

Credit card fraud can pose a significant risk for businesses that sell online.

SecurePay is committed to providing safe and secure online payment options. SecurePay Online Payments provides a highly secure Payment Card Industry Data Security Standard (PCI DSS) compliant solution. It ensures that customer credit card details are transmitted between your bank, the customer's bank and the credit card schemes in a highly secure manner.

KEEPING CREDIT CARD DATA SECURE

A customer's credit card data is among their most important personal information, so your customers must be certain that their data is secure.

The security of credit card data is mandated internationally by the Payment Card Industry Data Security Standard (PCI DSS). This is governed by the Payment Card Industry Security Standards Council.

Businesses have a responsibility to keep customer data secure. The easiest way to do this within the PCI DSS guidelines is not to transmit, process or store card data, and to use a compliant integration method from SecurePay.

With SecurePay, you never have any access to full customer credit card information or data. This helps to reduce your business risk and can help make customers feel more secure when they buy online from you.

HOW BUSINESSES BENEFIT FROM COMPLYING WITH SECURITY STANDARDS

Being PCI DSS compliant protects customers and helps minimise risk to your business. Here are some of the advantages:

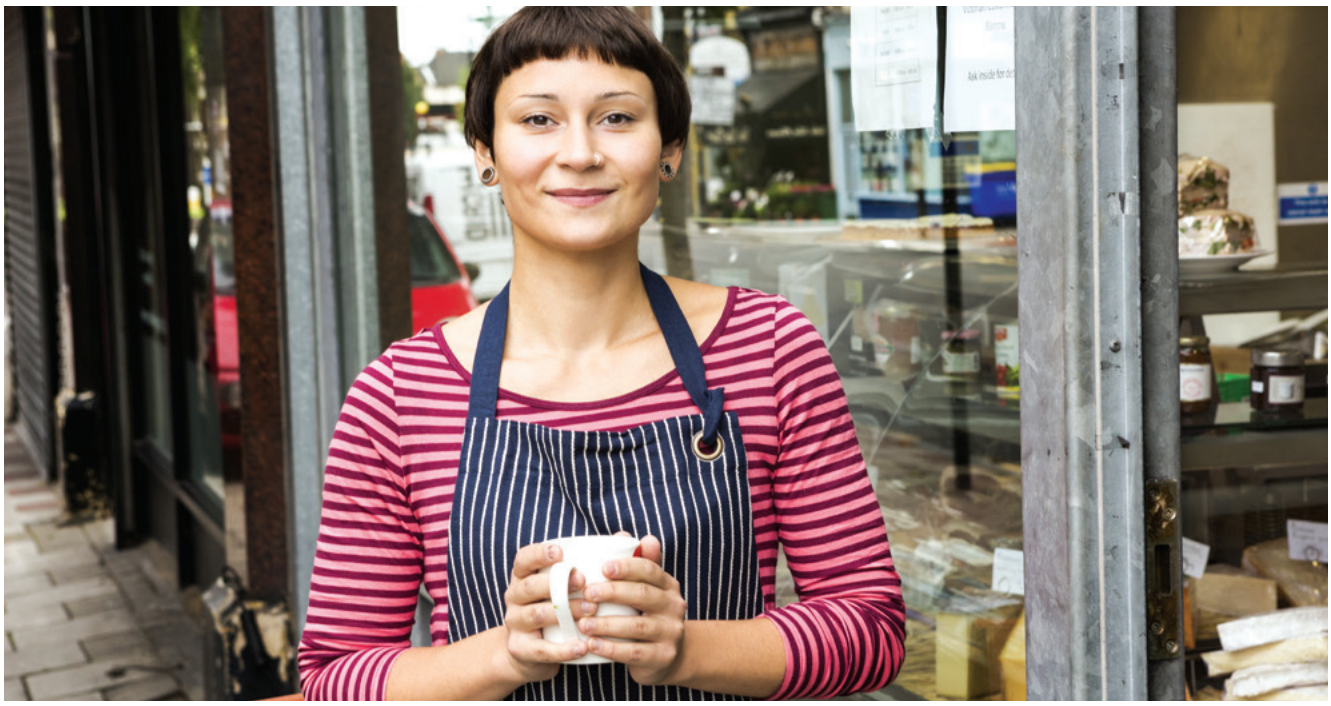
- Your customers' credit card data is protected.
- Checking that you are PCI DSS compliant is a "health check" for your business processes and systems.
- It reduces one of the significant risks for an e-commerce business.
- It helps protect your business reputation.
- It helps reassure customers that it's safe to shop online.

You can also take further security steps to protect yourself from credit card fraud, from monitoring transactions for suspicious activity, to third-party services that can help identify risky transactions.

10 SIGNS OF FRAUD

The following characteristics could indicate an increased risk of online fraud:

1. **First-time shopper:** Fraudsters are always looking for new e-commerce businesses to defraud.
2. **Larger-than-normal orders:** Stolen cards or account numbers have a limited life span, so thieves need to maximise the size of their purchases.
3. **Ordering multiples of the same item:** Having variants of the same item (such as different sizes or colours) can increase a fraudster's profits on resale.
4. **Express or overnight shipping:** The sooner the fraudster receives the order, the sooner they can resell the items. Also, you may have despatched the order before you discover it is fraudulent.
5. **Multiple transactions on one card over a very short time:** This could be an attempt to "run" a card until the account is closed.
6. **Inconsistencies:** Keep an eye out for different billing and shipping addresses, telephone codes that don't match postcodes, email addresses that don't look legitimate and orders placed at unusual times.
7. **Multiple cards with a single delivery address:** Account numbers could have been generated using special software, or it could indicate a batch of stolen cards.
8. **Multiple transactions on one card or a similar card with a single billing address, but with multiple shipping addresses:** This could be organised activity by a group of fraudsters.
9. **Multiple cards but a single IP address:** More than one or two cards could indicate a fraud scheme.
10. **Orders from internet addresses that use free email services:** Free email services don't require billing, so there is often no audit trail and no way to check that a legitimate cardholder has opened the account.



EXTRA LEVELS OF SECURITY

E-commerce businesses can use a combination of tests and strategies to assess the risk of a transaction, determine the validity of a customer and accept or reject an order. Many of these tests can be conducted automatically with fraud-prevention products and systems.

Instead of manually reviewing each order, it's usually more cost effective to have automated internal screening or to engage a third-party tool, like one from SecurePay, to screen for questionable transactions.

COMBAT SUSPICIOUS TRANSACTIONS WITH SECUREPAY FRAUDGUARD

SecurePay also offers FraudGuard to help you detect fraudulent transactions before they occur. With FraudGuard, you set up your own fraud-screening rules, using a points system to allow you to completely customise your fraud settings. If the Fraud Score exceeds 100, then the transaction will be flagged as fraudulent. You can set up FraudGuard to send you an email alert and / or block the transaction when it has been flagged as fraudulent.

TWO EASY WAYS TO COMBAT FRAUD:

1 ASK THE CARDHOLDER FOR THE THREE OR FOUR-DIGIT CARD VERIFICATION VALUE (CVV).

The CVV is printed on Visa, MasterCard and American Express cards. This is also sometimes called CVV2 or CVN.

- All e-commerce transactions must include the CVV. (An e-commerce transaction is defined as a payment accepted over the internet, where the cardholder is entering the card details themselves.)
- To maintain the security of the card, it's important that the CVV is not stored in your system.
- Asking for the CVV may help you to verify that the person placing the order has the actual card in their possession.

2 USE YOUR OWN CUSTOMER HISTORY DATA.

- If you have had a fraudulent order with a customer, add the details of that transaction to you internal "negative lists".

CONTACT US

SecurePay is based in Australia, and our payment specialists are available to answer any questions you may have about the compliance process or online security. For more information, call 1300 656 372 or email: onlinepayments@securepay.com.au.

CONNECT WITH SECUREPAY ON:

SecurePay