



## Disclosure & Payment Compliance

How to Shape Policies That Gain Customer Confidence

PayPal Business Guide



# Introduction

Selling your products or services online is a great way to start a new business or extend an existing brick-and-mortar business. While the internet and digital technology are transforming commerce, some business basics haven't changed for thousands of years. The relationship between sellers and buyers has always been based on integrity and trust. Trust-building practices, such as personal contact and handshake agreements, are impossible with the internet, but there are ways to communicate honesty and security to your customers while building long-term success.

**Make your customers feel secure by telling them about your business practices and what you plan to do with the financial information they give you.**

With your online business, you'll likely be accepting credit and debit card payments and managing names, addresses, phone numbers, email addresses, credit or debit card numbers, and other financial information. You'll want to make your customers feel secure by telling them about your business and business practices, as well as what you plan to do with the personal and financial information they give you. That's what your "disclosure policy" is all about.

Your other responsibility to your customers is to ensure that this personal and financial data is protected. An industry standard known as Payment Card Industry (PCI) Data Security Standard was adopted in 2004 as the result of a collaboration between the various card associations to protect customer information. As a merchant that stores, processes, and transmits credit card data you – and your service providers – are required to comply with this payment standard. Like your disclosure policy, your compliance with PCI helps build good relationships with your customers.

# Disclosure Policy – What You’ll Want to Tell Your Customers

Your disclosure policy tells your customers that you’re honest and dependable – and that you care about them and protecting their information. It shows your customers that you believe in transparency and accountability. It provides a framework and standards for your business policies, how you deal with your customer information, and how you communicate with your customers.

Your disclosure policy typically includes five things: a business description, privacy policy, delivery policy, return, refund and cancellation policy and contact information. The more your customers know about you, the more comfortable they’ll be giving you their business. So be honest, open, direct, and precise.

Your disclosure policy typically includes:

- Business description
- Privacy policy
- Shipping policy
- Return policy
- Contact information

Here are more details about the five areas you should cover:

1. **Business description.** This is simple enough. Write a clear description of what your company does, including what products and services it provides. Post it in a prominent place on your website, often the “About Us” section.

Here is an example, using PayPal’s [business description](#).

2. **Privacy policy.** Your privacy policy should clearly state how you treat and protect your customers’ information. It’s essential that your policy is easy to find on your website, usually linked from your homepage. Typical elements of a privacy policy include:

- What personally identifiable customer information you collect
- How the information is used
- With whom you share and do not share this information
- What choices are available to your customers regarding collection, use, and distribution of the information
- What choices are available to your customers regarding communications from you – email, direct mail, etc.
- The kind of security procedures in place to protect the loss, misuse, or alteration of information under your control
- How your customers can correct any inaccuracies in the information

For simplicity, it is recommended you confirm clearly whether or not you intend to store or currently store financial details (credit or debit card numbers). There are also legal requirements which apply to privacy disclosures and we strongly suggest you obtain legal advice when preparing this policy. See our section below on safeguarding your customers personal information for further details.

Here is an example, using PayPal’s [privacy policy](#).

3. **Delivery policy.** You've made the sale. Your customers are anxious to get their purchases. So keep that excitement and positive momentum going with a delivery policy that's simple and straightforward:

- Spell out your delivery terms in detail, disclosing if costs are determined by weight or the amount of the purchase
- Indicate the types of delivery you offer - ground, express, overnight, etc.
- Indicate where you deliver to, or do not deliver to
- Tell your customers in what timeframe they can expect their purchase
- Show your customers how they can track their shipment. (Your distributors should be able to provide most of this information for you.)

4. **Return / Refund / Cancellation policy.** Your customers love simplicity – and forgiveness. They sometimes make mistakes and order the wrong products. They may be unfamiliar with what they are ordering and it's not what they had in mind. By allowing your customers to return or cancel an item in a timely fashion – and making it easy to do so – you are gaining their loyalty. A clear return and refund policy also comes in handy if the order arrives damaged. So make it easy for them to initiate returns:

- Spell out exactly what your return policy is, for example that you accept returns only as exchanges or you accept returns and will credit their payment card
- Be specific about how many days after purchase the item can be returned in order to get a refund or exchange
- Let them know if you charge a restocking fee on returns
- Include a return shipping label with every order
- Include your customer service number or email address in case customers have questions or comments.
- Provide clear return instructions, such as asking for a reason for the return and a telephone number in case you have questions
- In the event that an order is cancelled make sure you specify your terms and conditions in this regard clearly

By allowing your customers to return an item in a timely fashion – and making it easy to do so – you are gaining their loyalty.

5. **Contact information.** Keep the channels of communication open. Make it easy to your customers to get in touch with you:

- Give examples of reasons they may want to contact you, for example questions about privacy policy, return policy, availability of goods, etc.
- Provide a phone number, and give the days and hours the phone lines are answered
- Provide an email address, and give a timeframe when an answer can be expected
- Provide a mailing address, and suggest to whose attention it should be Addressed

Here is an example, using PayPal's [contact information](#).

Now you have the framework for conducting better online business, make sure you clearly update your website or business brochure with the policies above. Simple, easy navigation to policy information online will drive a better customer experience at the point of sale.

**Policies are also a vetting requirement for all Website Payments Pro and Virtual Terminal merchants:** Please be aware that, PayPal reserves the right to reassess your use of our products and services and may contact you for clarification on certain aspects of your business, prior to approval and/or once you have initiated your first transaction.

# Secure Payment Processing Ensures Customer Trust

PayPal's solutions provide secure, reliable payment connections among merchants, customers, and financial networks. Products including Website Payments Standard, Website Payments Pro and Virtual Terminal allow everyone from small online cottage industries to enterprise-level business to process transactions easily, reliably, and securely.

What's more, additional options will allow you to scale quickly and seamlessly as your business grows. PayPal's Fraud Protection Services and Recurring Billing Services, along with other customer service packages, include professional integration support.

PayPal's payment products allow everyone from small online cottage industries to enterprise level businesses to process transactions easily, reliably and securely.

Determining which product is right for you is a matter of asking a few simple questions:

## 1. Do you need an all-in-one solution that includes an internet merchant account and allows you to process credit cards online?

If you don't have your own internet merchant account, PayPal can provide a total solution with Website Payments Standard and Website Payments Pro.

**Website Payments Pro:** Website Payments Pro is an all-in-one payment solution that allows customers to shop and pay on your site. You can accept credit cards directly on your site, or through a virtual terminal, and get the features of a merchant account and gateway through a single provider at a lower cost. Website Payments Pro allows you to control your checkout from start to finish.

**Website Payments Standard:** Website Payments Standard lets customers shop on your website and pay on PayPal. It offers a pay-per-use model with no set-up or monthly fees. Like Website Payments Pro, it includes shipping and tax calculators, reporting tools to measure your business, and support for international currencies.

## 2. Do you prefer to accept phone, fax and email orders ?

**PayPal Virtual Terminal:** Virtual Terminal provides your business with the same functionality as a stand-alone, credit card-processing terminal by allowing you to accept credit card payments by phone, fax, and email. You can use Virtual Terminal on any computer with an internet connection.

For demonstrations of all PayPal's payment solutions and additional information, visit <https://www.paypal.com/uk/ukmerchant>. Alternatively view:

[Website Payments Pro Demo](#)

[Website Payments Pro PDF](#)

[Website Payments Standard Demo](#)

[Virtual Terminal](#)

# Payment Compliance – Safeguarding Your Customers’ Account Information

Just as a disclosure policy describes your business and states your business practices, your compliance with the PCI Data Security Standard [see chart below] communicates how much you care about your customers and reinforces an atmosphere of safety for all online merchants.

PCI data security compliance assures your customers that you’re looking out for their safety and well-being.

Consumers are becoming increasingly aware of the dangers of identity theft due to compromised data and stolen credit card information. PCI compliance assures your customers that you’re looking out for their safety and well-being. Approach it with that in mind, and you transform compliance into a competitive edge and asset instead of a dreaded “must do.”

Today, virtually all major credit card companies, including MasterCard International®, and Visa® require merchants and service providers to comply with the PCI standard. When you process credit card transactions through a merchant account, you also need to meet PCI validation requirements, including quarterly and annual audits, security self-assessments, and security scans. Your exact validation requirements are determined by your volume of credit card transactions.

While validating that you’re in compliance with the PCI standard is a requirement [see chart on page 8], it’s also an opportunity. Finding and fixing compliance gaps before your audit keeps your company running smoothly and your reputation intact. It provides you with tangible proof that you can communicate to your customers on how well you’re protecting them.

The quickest and easiest way to meet PCI compliance standards is to outsource the job. A number of PayPal payment solutions are hosted, relieving the online merchant of the compliance responsibility.

Get more information about the [PCI Security Standards Council](#).

## PCI Data Security Standard

| Standards                                   | Requirements  |
|---|---|
| Build and Maintain a Secure Network         | 1. Install and maintain a firewall configuration to protect data.<br>2. Do not use vendor-supplied defaults for system passwords and other security parameters.       |
| Protect Cardholder Data                     | 3. Protect stored data.<br>4. Encrypt transmission of cardholder data and sensitive information across public networks.   |
| Maintain a Vulnerability Management Program | 5. Use and regularly update antivirus software.<br>6. Develop and maintain secure systems and applications.   |
| Implement Strong Access Control Measures    | 7. Restrict access to data by business need-to-know.<br>8. Assign a unique ID to each person with computer access.<br>9. Restrict physical access to cardholder data. |
| Regularly Monitor and Test Networks         | 10. Track and monitor all access to network resources and cardholder data.<br>11. Regularly test security systems and processes.                                      |
| Maintain an Information Security Policy     | 12. Maintain a policy that addresses information security.  |

### Merchant levels for PCI compliance

The compliance level of each merchant is the responsibility of the merchant's acquiring bank (a bank that provides credit card merchant accounts and is responsible for submitting credit card purchase information to the credit card associations). The four merchant levels are based on annual credit card transaction volume.

|         |  |
|---------|--|
| Level 1 | Any merchant – regardless of acceptance channel – processing over 6 million credit card transactions per year.<br>Any merchant that has suffered a hack or an attack that resulted in an account data compromise.<br>Any merchant identified by any card association as Level 1. |
| Level 2 | Any merchant processing 150,000 to 6 million e-commerce transactions per year.   |
| Level 3 | Any merchant processing 20,000 to 150,000 e-commerce transactions per year.  |
| Level 4 | Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants processing up to 6,000,000 credit card transactions per year.  |

### PCI compliance validation requirements

In addition to adhering to the PCI Data Security Standard, compliance validation is required for Level 1, Level 2, and Level 3 merchants, and may be required for Level 4 merchants.

|               | Validation Action   | Validated By   |
|---------------|---|--|
| Level 1       | Annual Onsite PCI Data Security Assessment<br>and<br>Quarterly Network Scan | Qualified Data Security Company or Internal Audit if signed by Officer of the company<br><br>Qualified Independent Scan Vendor |
| Level 2 and 3 | Annual PCI Self-Assessment Questionnaire<br>and<br>Quarterly Network Scan   | Merchant<br><br>Qualified Independent Scan Vendor  |
| Level 4*      | Annual PCI Self-Assessment Questionnaire<br>and<br>Quarterly Network Scan   | Merchant<br><br>Qualified Independent Scan Vendor  |

\*Level 4 merchants must comply with the PCI Data Security Standard; however, compliance validation for merchants in this category is determined by the merchant's acquirer.

# Payment Compliance – Safeguarding Your Customers' Personal Information

Now you have reviewed your PCI Compliance responsibilities, informing your customers about how their personal information is stored or handled, in accordance with the Data Protection Act, is your next step. Like PCI Compliance, clear, concise detail on your Data Protection practices will reinforce your customer relationships and foster an environment of trust. It is also a legal requirement as all organisations must make sure that they comply with the Data Protection Act.

**The Data Protection Act gives your customers the right to know what information is held about them, and sets out rules to make sure that you handle this information properly.**

The Data Protection Act has a number of important applications but primarily it works in two ways:

**1. It gives your customers the right to know what information is held about them, and sets out rules to make sure that this information is handled properly.**

Should an individual or organisation feel they're being denied access to personal information they're entitled to, or feel their information has not been handled according to the eight principles, they can contact the Information Commissioner's Office for help. Complaints are usually dealt with informally, but if this isn't possible, enforcement action can be taken.

**2. It requires all organisations which handle personal information to comply with eight important principles regarding privacy and disclosure.**

Anyone who processes personal information must make sure that customers personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

Get more information about the [Data Protection Act \(1988\)](#).

# Beyond Payment Security and Compliance: What PayPal Is Doing to Protect Your Business Against Fraud

The security of your information, transactions, and money is the top priority at PayPal. PayPal Fraud Protection Services leverages the Secure Sockets Layer (SSL) protocol, which provides crucial online identity and security to help establish trust between parties involved in e-commerce transactions. Your customers can be assured that the website they're communicating with is genuine and that the information they send through web browsers stays private and confidential.

**PayPal's proprietary risk models help detect and predict fraudulent transactions – before they affect your business.**

Moreover, using SSL with an encryption key length of 128 bits (the highest level commercially available), PayPal automatically encrypts your confidential information in transit from your computer to PayPal's servers, which are heavily guarded both physically and electronically. These servers sit behind a monitored electronic firewall and are not connected directly to the internet, so your private information is available only to authorized computers.

PayPal also helps protect your business against fraud, so you can grow while minimizing losses. Proprietary risk models help detect and predict fraudulent transactions – before they affect your business. Industry-recognized address verification system (AVS) and card security code checks thwart identity theft. Patent-pending bank account verification adds an additional level of authentication. Verification gives you more information about the people with whom you transact through PayPal, so you can make more informed decisions.

Get more details about ways to [sell safely and prevent fraud](#).

# Additional Resources About Disclosure and Compliance

There are other online resources that can help you in developing your own disclosure policy and meeting PCI compliance and Data Protection Act requirements.

They include:

- The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection:  
<https://www.pcisecuritystandards.org/>
- The Information Commissioners Office is the UK's independent authority set up to promote access to official information and to protect personal information :  
<http://www.ico.gov.uk/>
- The Office of Fair Trade offers valuable information on selling to consumers online, and the Distance Selling Regulations that may apply to you:  
[http://www.offt.gov.uk/advice\\_and\\_resources/small\\_businesses](http://www.offt.gov.uk/advice_and_resources/small_businesses)
- Both the Visa and MasterCard websites have extensive information about meeting PCI Payment Data Security Standards:  
<http://www.visaeurope.com> and <http://www.mastercard.com/uk>

Remember that PayPal is always available to answer your questions and provide guidance on compliance best practices for your e-commerce site. For more information, visit the PayPal site at <https://www.paypal.co.uk> and follow the Business and Merchant Services links.

PayPal Business Guide – Disclosure & Compliance

© 2008 PayPal, Inc. All rights reserved. PayPal and the PayPal logo are registered trademarks of PayPal, Inc. Designated trademarks and brands are the property of their respective owners.

## Notice of Non-Liability

PayPal, Inc. and the authors assume no liability for errors or omissions, or for damages, resulting from the use of this guide or the information contained in this guide.