# Challenges

As an eCommerce business, you are responsible for protecting your customers' payments data. As hackers become more organized and sophisticated, the need to protect this vital information is more imperative than ever.

By accepting cardholder data, you must address the risks of becoming a target for sophisticated cybercriminals — your customers expect you to appropriately protect their data from these attacks. Failure to do so can result in data compromise which comes with devastating fines, fees, disclosure requirements, lawsuits, and serious loss of trust with your customers.

Revisions to PCI DSS guidelines for eCommerce environments may still require organizations to validate new PCI controls, even though they outsource to a PCI-certified third party. This often results in higher compliance obligations and annual expenditures. Additionally, these certified third parties may not be able to transfer the entire risk of capturing cardholder data as the business is still liable until the cardholder data arrives at their acquirer.

**Worldpay eProtect:**
A comprehensive data security solution

The best way for businesses to reduce the impact of a data compromise is for their systems to never have access to the cardholder data at all.

Worldpay eProtect is a comprehensive card-not-present data security service that immediately captures cardholder data upon entry into your online checkout page. It then replaces this data with a dynamically generated tokenized value that can only be used by you for payment processing, but is useless to criminals and unauthorized parties.

To capture sensitive payment data in alignment with PCI standards, Worldpay eProtect utilizes a fully-customizable iFrame element that fits smoothly within your web page and is hosted in Worldpay's secure environment, transferring the risk to Worldpay. This approach reduces the risk and the scope of your PCI compliance responsibilities with minimal impact to your systems and operations. Plus, the hosted payment fields can replicate the existing style and layout of your website, resulting in a richer experience for your customers.
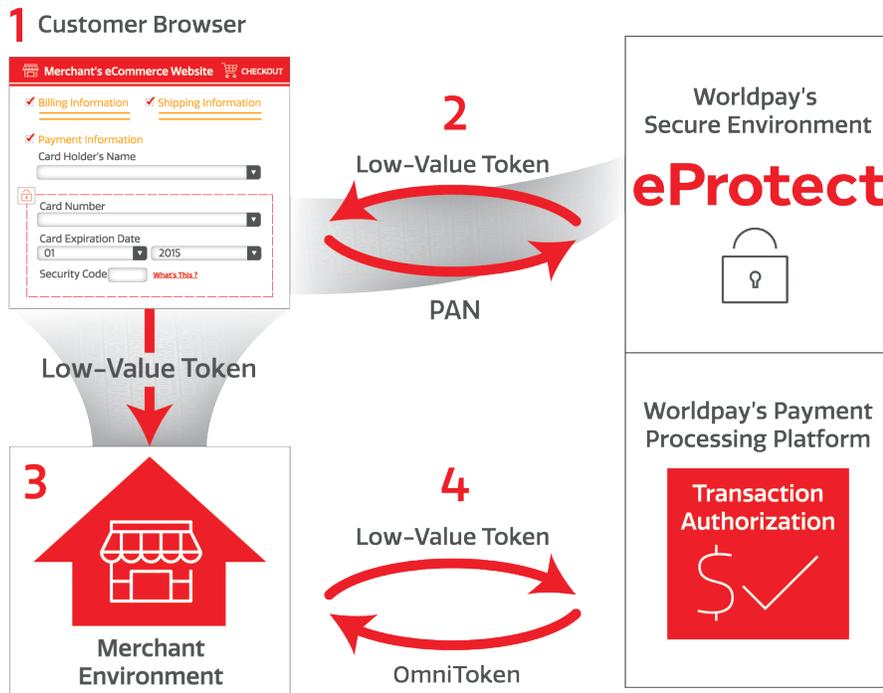
For storage of cardholder data, Worldpay OmniToken values are utilized for all post-authorization operations, and can be safely stored throughout your systems with no risk of data theft.

Since cardholder data never enters your systems, and only Worldpay has access to sensitive cardholder data, eProtect effectively transfers the risk of capturing and storing cardholder data from you to us.
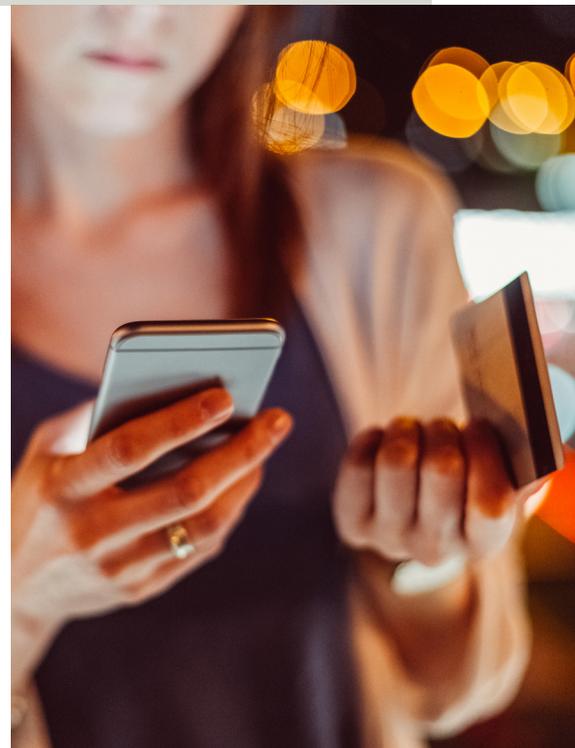
**To learn more how Worldpay eProtect can help you secure and protect your data, please call 844.843.6111, Option 2.**

## How Worldpay eProtect Works

**1** Customer Browser

Merchant's eCommerce Website — CHECKOUT

✔ Billing Information    ✔ Shipping Information

✔ Payment Information
Card Holder's Name

Card Number

Card Expiration Date
01    2015

Security Code    What's This ?

**Low-Value Token**

**3**

Merchant
Environment

**2**

Low-Value Token

PAN

**4**

Low-Value Token

OmniToken

Worldpay's
Secure Environment

**eProtect**

Worldpay's Payment
Processing Platform

Transaction
Authorization

$✓

**1** When a customer is ready to enter their cardholder data into your web page, your web server delivers a form to the customer's web browser and loads the iFrame hosted by the Worldpay eProtect server.

**2** The customer enters their payment information into the iFrame fields and clicks the Submit button on your page which then calls the eProtect server, returning a single-use low-value token. The payment information is then forwarded to Worldpay's data security platform and held until authorization request.

**3** Your web page submits the low-value token and non-cardholder data elements to your web server for order processing.

**4** Once the authorization request arrives at Worldpay's payment processing platform, the low-value token is detokenized, converted to a high-value token — Worldpay's OmniToken — and returned to you along with the authorization response.

## Worldpay eProtect Features

· **Card Verification Code Capture** – eProtect not only securely captures sensitive data from first-time guests, it also captures the Card Security Code (CVV2) as a standalone data element for card-on-file and non-recurring purchases. This data element is replaced by a dynamically-generated token, which removes the responsibility for capturing sensitive authentication data out of your hands, and helps tackle account takeovers (ATOs) and other fraudulent activities targeting card-on-file payments.

· **Enhanced eProtect iFrame Design** – Simplify the payment capture experience by using our streamlined and customizable iFrame. Real-time user validation improves online conversions, decreases human errors, and helps improve the customer buying experience.

· **Interoperability** – Integrates seamlessly with all core processing transactions, including authorizations, deposits, sales, refunds, chargebacks, etc. Token values also work seamlessly with many of Worldpay's value-added services, including Account Updater, Authorization Recycling, Fraud Toolkit, Chargeback Prevention, and Issuer Insights.

WEC023 10.18