ONLINE MERCHANT SECURITY

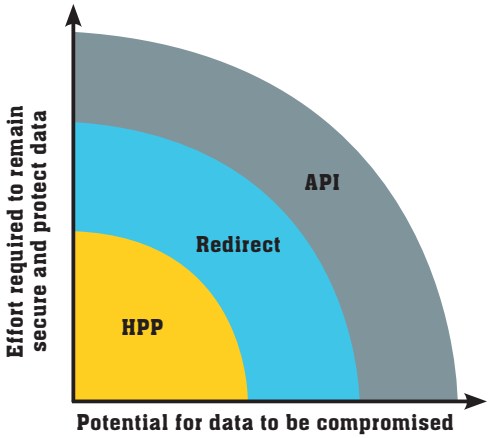
Understand your obligations and ensure you protect cardholder data.

Reduce your business's exposure to online payment fraud and free your business from security concerns, by implementing the highest industry security standards available. Partner with the Commonwealth Bank to protect your business and your customers from fraud by following these simple steps.

Step 1:
Choose the right online solution for your business

Online solutions vary in the level of control the merchant has over the end-to-end consumer experience and, the effort required by the merchant to adequately protect cardholder data collected from consumers.

Common online solutions and their respective security considerations are outlined in the graph and below.



HPP

Recommended By CommBank

BPoint Internet, Hosted Payment Page (HPP), 3-Party hosted, i-Frame or Lightbox

Cardholder data is captured by your Bank or a compliant service provider (such as a Payment Gateway) on pages that are integrated into your website, but don't reside there.

This reduces the amount of information held in your environment, and allows you to achieve and maintain compliance with minimal effort and investment.

Redirect

BPoint Payment Connector, 302 Redirect or Direct Post

Cardholder data is captured by your website and is redirected to your Bank or a compliant service provider, (such as a Payment Gateway) at the point of submitting the payment/s.

This reduces the amount of information held in your environment, and allows you to achieve and maintain compliance with moderate effort and investment.

API

Application Programming Interfaces (APIs) including BPoint, Payment Gateway or 2-Party merchant hosted

Cardholder data is captured by your website and is submitted to your Bank or a compliant service provider (such as a Payment Gateway) but resides on your server(s), connected systems and infrastructure.

This increases the amount of information held in your environment, and requires a high level of effort and investment to achieve and maintain compliance. If not protected, cardholder data in this environment is most susceptible to compromise.

CAN

Step 2:
Understand your obligations to protect cardholder data

As a merchant you have access to cardholder data entrusted to you by your customers. An important condition of your merchant agreement is that you use, manage and store cardholder data in line with global security best practices, known as the Payment Card Industry Data Security Standard (PCI DSS). Meeting PCI DSS requirements minimises the chances of you suffering from a compromise, and reduces the risk of reputational damage, financial losses and potential negative publicity to your business.

For more information about your obligations, please visit www.commbank.com.au/merchantagreement

---

Step 3:
Achieve compliance

Protect your business and customers by achieving compliance with the PCI DSS. For information about the PCI DSS, Self Assessment Questionnaires and Vulnerability Scans, visit the Payment Card Industry Security Standards Council (PCI SSC) website at www.pcisecuritystandards.org/merchants. Validation requirements for the various online solutions are outlined in the table below.

Online Solution	Self Assessment	Vulnerability Scan
BPoint Internet, Hosted Payment Page (HPP), 3-Party hosted, i-Frame or Lightbox	✔	–
BPoint Payment Connector, 302 Redirect or Direct Post	✔	✔
Application Programming Interfaces (APIs) including BPoint, Payment Gateway or 2-Party merchant hosted	✔	✔

Important information: As this advice has been prepared without considering your cardholder data environment, you should before acting on the advice, consider its appropriateness to your circumstances and understand your ongoing obligations to maintain compliance with the PCI DSS.

CAN