Processing e-commerce payments

A guide to security and PCI DSS requirements

August 2014

VISA

Contents

Processing e-commerce payments

A guide to security and PCI DSS requirements

There are a number of ways to secure e-commerce transactions. How a website asks for the payment data and what happens to the data once the customer clicks 'OK' can affect the security of the transaction.

This guide:

- Shows the various common ways that websites ask for payment card data.
- Describes the PCI DSS requirements of the merchant's website.
- Explains how criminals try to disrupt the payment flow to capture cardholder data.

Foreword by Peter Bayley

Wherever cardholder data is processed, criminals will try to find ways to steal that data to commit fraud. In the past three years we've seen many innovative ways that merchants have chosen to process cardholder data for e-commerce transactions. The criminals have also noticed that some of these new methods of processing data are easier to compromise than others.

The Payment Card Industry Security Standards Council recently released PCI DSS version 3.0 along with a new self-assessment questionnaire for some e-commerce merchants (SAQ A-EP). A number of the changes in this new version of DSS have been introduced to help acquirers, merchants and their Qualified Security Assessors secure cardholder data in an online environment. The new standard can be used today, and is mandatory from the start of 2015.

I understand that when new versions of the standards are released, it can cause confusion and may influence merchants to change the way they process transactions. Visa Europe has produced this guide to explain the minimum requirements we expect of merchants to secure cardholder data and how merchants should report their PCI DSS compliance to an acquiring bank. We've illustrated the cardholder data flow for typical e-commerce transaction architectures, described the risks and stated our compliance requirements for each one. I hope this helps your understanding of the new standards and the risks associated with processing cardholder data.

Peter Bayley
Executive Director, Risk Management

"In the past three years we've seen many innovative ways that merchants have chosen to process cardholder data for e-commerce transactions."

The systems involved

Three computer systems are involved whenever a customer makes a card purchase on the internet.

The merchant website
Contains the product catalogue and shopping cart. Always starts the process to collect the customer's cardholder data when the customer asks to checkout.

The customer computer
Running a web browser such as Firefox, Chrome or Internet Explorer.

The payment service provider (PSP)
A Visa Europe listed validated PCI DSS compliant company that receives the cardholder data and submits it to the payment system.

The key steps involved

There are three key, separate steps in collecting a payment from the customer; the way that these are designed will affect the security of the transaction.

Step 1.
CREATE the payment form to collect the customer's card data and SEND the payment form to the customer computer. This can be done by the merchant website, or by the PSP website.

Step 2.
The customer computer displays the payment form, and the customer enters their card data and presses the OK button (often called 'submit' or 'pay now') to confirm the payment, which tells the customer computer to SEND the card data to the PSP or to the merchant website. This step always happens on the customer computer.

Step 3.
RECEIVE the card data entered by the customer into the payment form and then send it to the payment system for authorisation. This can be done by the merchant website, the PSP or both the merchant website and the PSP working together.

This guidance document will look at the various ways that companies do this today, and explain how each works and identify the systems that make each step happen.

Important notes

- Some of the technical details of how this happens have been simplified, to concentrate on the flows of payment forms and cardholder data.
- All communications between the customer computer, the merchant website and the PSP must be encrypted.

The Payment Card Industry (PCI) Data Security Standard (DSS)

PCI DSS describes the way that merchants and PSPs should secure their systems. PCI DSS applies to all merchants that accept Visa cards and the number of technical requirements that apply depend on which way the merchant configures their website to accept card payments. PCI DSS applies to all merchants' webservers, even if a webserver does not itself store, process or transmit cardholder data because the merchant's webserver determines how cardholder data is processed and so can affect the security of the transaction.

There are two ways a merchant can validate its compliance with PCI DSS – by completing a self-assessment questionnaire (SAQ) or by obtaining a Report on Compliance (RoC) using a PCI Security Standards Council registered Internal Security Assessor (ISA) or Qualified Security Assessor (QSA).

There are three options:

	SAQ A / RoC[A]	SAQ A-EP / RoC[A-EP]	SAQ D / RoC
Criteria	The entire payment page is received from and returned to a Visa Europe listed validated PCI DSS compliant third party provider.	The merchant website does not store, process or transmit cardholder data but controls how the data is collected.	The merchant website stores, processes or transmits cardholder data.
Requirements	Merchants must ensure they use only Visa Europe listed validated PCI DSS compliant third party providers.	A sub-set of PCI DSS requirements designed to protect the integrity of the merchant's webserver and that Visa Europe listed validated PCI DSS compliant third parties are used.	All PCI DSS requirements are applicable.

Visa Europe has different minimum requirements for e-commerce merchants depending on how they accept cardholder data and the number of Visa card transactions they process annually. Merchants should contact their acquiring bank to confirm the validation method they need to use. The risk to cardholder data and the validation requirements are based solely on the actual types of attacks that Visa Europe is seeing against merchants.

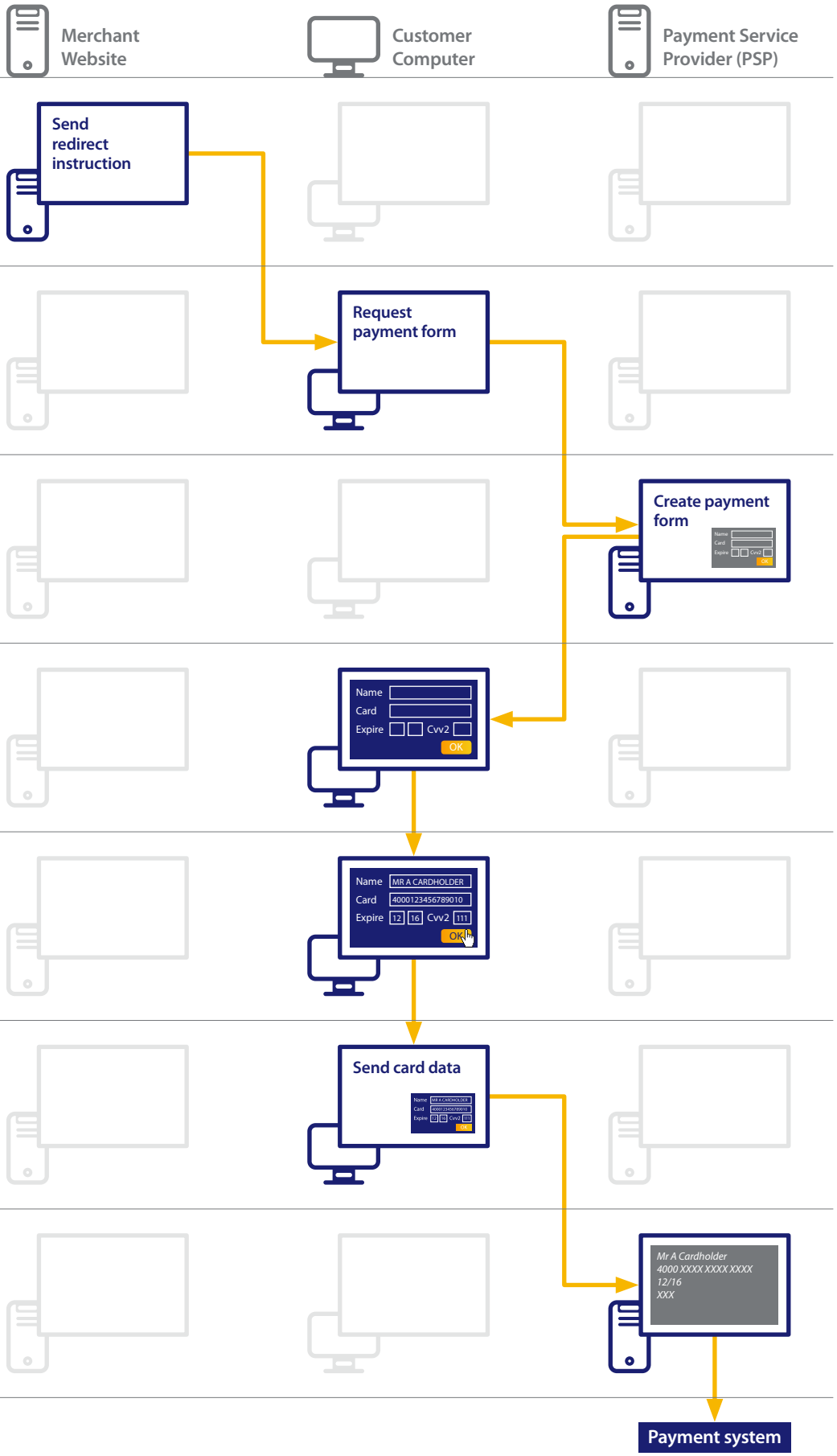
The following table summarises the validation requirements from January 1st 2015. Merchants who meet the validation requirements will be granted safe harbour from penalties in the event of an account data compromise.

Merchant Level	No of Visa Transactions Annually	Redirect	IFRAME	Direct Post	JavaScript	XML	Anything else
1	Over 6 million	RoC[A]	RoC[A]	RoC[A-EP]	RoC[A-EP]	RoC	RoC
2	1– 6 million	SAQ A	SAQ A	SAQ A-EP	SAQ A-EP	SAQ D	SAQ D
3	20,000 – 1 million	SAQ A	SAQ A	SAQ A-EP	SAQ A-EP	SAQ D	SAQ D
4	Under 20,000	SAQ A	SAQ A	SAQ A-EP	SAQ A-EP	SAQ D	SAQ D

RoC[A] – Partial Report on Compliance validating the scope, eligibility and requirements listed in SAQ A
RoC[A-EP] – Partial Report on Compliance validating the scope, eligibility and requirements listed in SAQ A-EP

The redirect process

When the customer wants to check out:



The redirect process

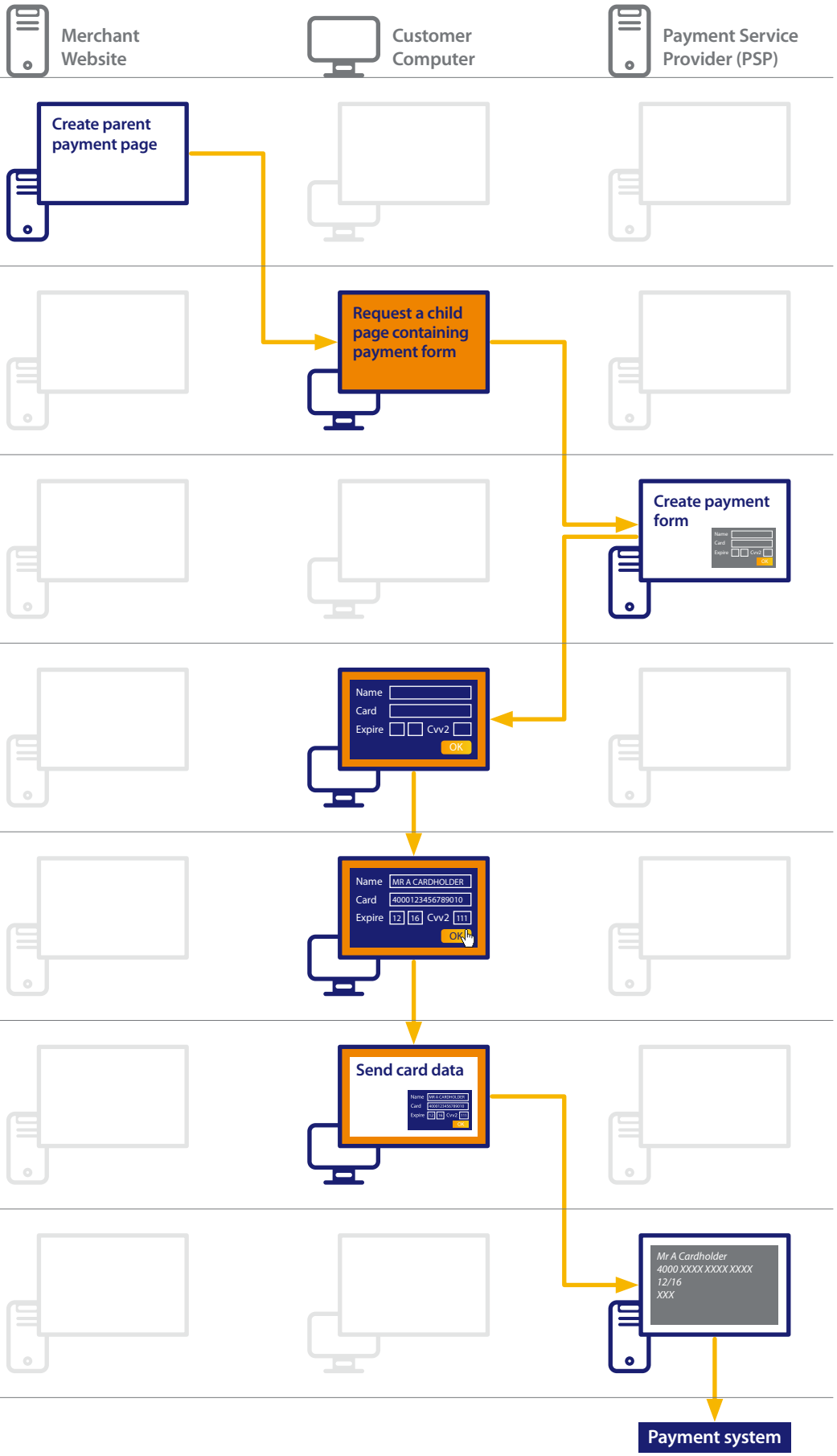
When criminals attack the redirect	
How	Criminals break the security of the merchant website and they change the program that sends the redirect instruction to the customer computer. This tells the customer computer to request a payment form from the criminal website instead of the PSP. The card data entered by the customer it is sent to the criminal and not to the PSP. Sometimes the criminal website collects the card data and sends it onto the PSP, sometimes the criminal website gets the card data and then tells the customer that there's been a problem and sends an instruction to the customer computer to now get the 'real' payment form from the PSP. This is known as a man-in-the-middle (MITM) attack.
What will the customer see?	The criminal payment form, which will be designed to look identical to the PSP payment form and may also ask for other information such as the card holder's PIN. Depending on how the criminals attack, the customer may be asked to enter their card data twice.
What will the merchant see?	The merchant may see a loss in sales caused by an increased transaction drop-out as customers are not taken in by the criminal's payment form or they don't want to enter their card data twice.
How can the merchant detect this attack?	The merchant should follow the Visa Europe guidance that explains how to detect and protect against this attack.

What level of PCI DSS compliance is required for the e-commerce channel?				
Merchant	Level 1	Level 2	Level 3	Level 4
	RoC[A]	SAQ A	SAQ A	SAQ A
PSP	A Visa Europe listed validated PCI DSS compliant service provider.			

Risk rating
Low – this method of processing e-commerce payments is the lowest risk for the merchant.

The IFRAME

When the customer wants to check out:



The IFRAME

When criminals attack the IFRAME	
How	The attack against the IFRAME is very similar to the attack against the redirect. Criminals break the security of the merchant website and they change the program that creates the parent page sent to the customer computer. Instead of the instruction telling the customer computer to request a CHILD page containing a payment form from the PSP, the instruction tells the customer computer to request a payment form from the criminal web site. So when the customer enters their card data it is sent to the criminal website and not the PSP. Sometimes the criminal website collects the card data and sends it onto the PSP, sometimes the criminal website gets the card data and then tells the customer that there's been a problem and sends an instruction to the customer computer to now get the 'real' payment form from the PSP. This is known as a man-in-the-middle (MITM) attack.
What will the customer see?	The criminal payment form, which will be designed to look identical to the PSP payment form and may also ask for other information such as the card holder's PIN. Depending on how the criminals attack, the customer may be asked to enter their card data twice.
What will the merchant see?	The merchant may see a loss in sales caused by an increased transaction drop-out as customers are not taken in by the criminal's payment form or they don't want to enter their card data twice.
How can the merchant detect this attack?	The merchant should follow the Visa Europe guidance that explains how to detect and protect against this type of attack.

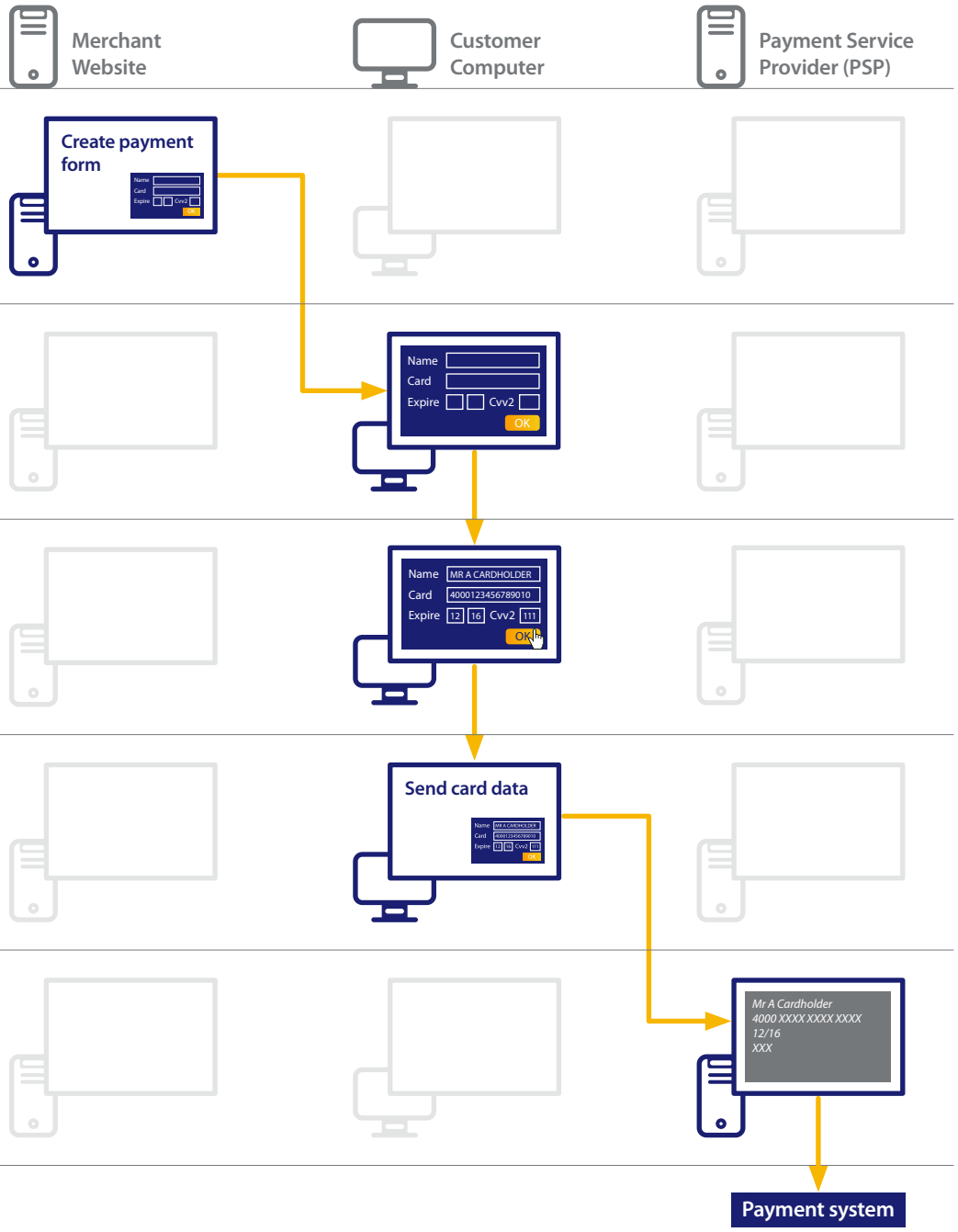
What level of PCI DSS compliance is required for the e-commerce channel?				
Merchant	Level 1	Level 2	Level 3	Level 4
	RoC[A]	SAQ A	SAQ A	SAQ A
PSP	A Visa Europe listed validated PCI DSS compliant service provider.			

Risk rating
Low – this method of processing e-commerce payments is low risk although it is more frequently attacked by criminals than the redirect process. Merchants should ask their PSP about technical measures they can use to best secure an IFRAME.

The direct post

(this is sometimes also called 'browser API' or 'silent order post')

When the customer wants to check out:



The direct post
(this is sometimes also called 'browser API' or 'silent order post')

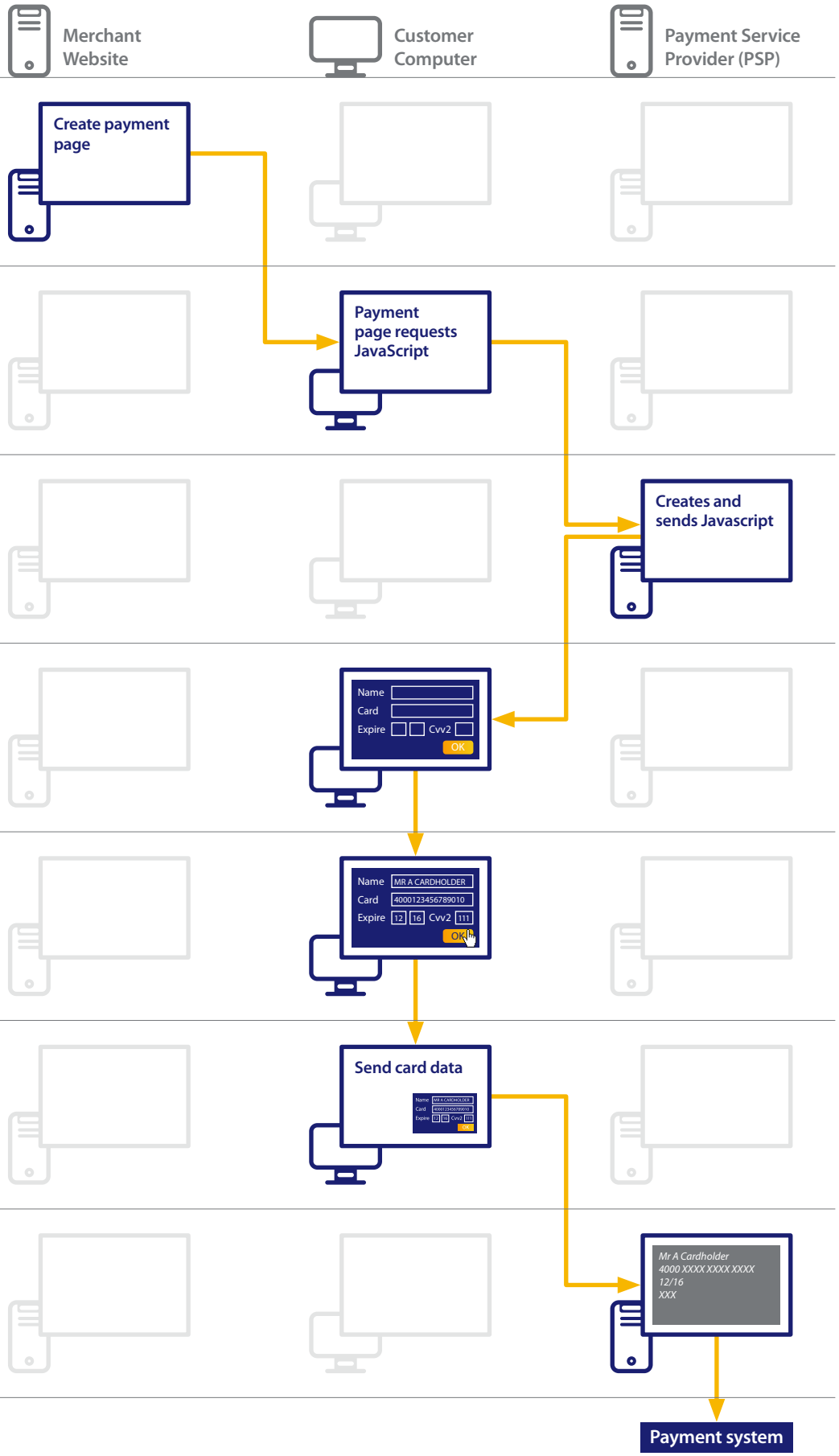
When criminals attack the direct post	
How	Criminals break the security of the merchant website and they change the program that creates the payment form. The criminals include some script so that when the customer enters the card data, it is automatically sent to the criminals as well as to the PSP.
What will the customer see?	The legitimate payment form. The customer will not notice the script running in the background which also sends the card data to the criminal.
What will the merchant see?	The merchant will not see any effects of this attack in their day-to-day operations.
How can the merchant detect this attack?	As detection by the merchant is very hard, the merchant should deploy the appropriate PCI DSS controls described in SAQ A-EP to help to prevent and detect this attack.

What level of PCI DSS compliance is required for the e-commerce channel?				
Merchant	Level 1	Level 2	Level 3	Level 4
	RoC[A-EP]	SAQ A-EP	SAQ A-EP	SAQ A-EP
PSP	A Visa Europe listed validated PCI DSS compliant service provider.			

Risk rating
Medium – this method of processing e-commerce payments is higher risk than the redirect process or the IFRAME and is currently being attacked by criminals.

The JavaScript created form

When the customer wants to check out:



The JavaScript created form

When criminals attack the direct post	
How	Criminals break the security of the merchant website and they change the program that creates the payment page that is sent to customer computer. The criminals change the page so as well as requesting some JavaScript from the PSP, the customer computer requests additional JavaScript from the criminal website so that when the customer enters the card data, as well as the card data being sent to the PSP, it is also sent automatically to the criminals.
What will the customer see?	The payment form. The customer will not notice the additional script running in the background of the payment form on the customer computer that also sends the card data to the criminal.
What will the merchant see?	The merchant will not see any effects of this attack in their day-to-day operations.
How can the merchant detect this attack?	As detection by the merchant is very hard, the merchant should deploy the appropriate PCI DSS controls described in SAQ A-EP to help to prevent and detect this attack.

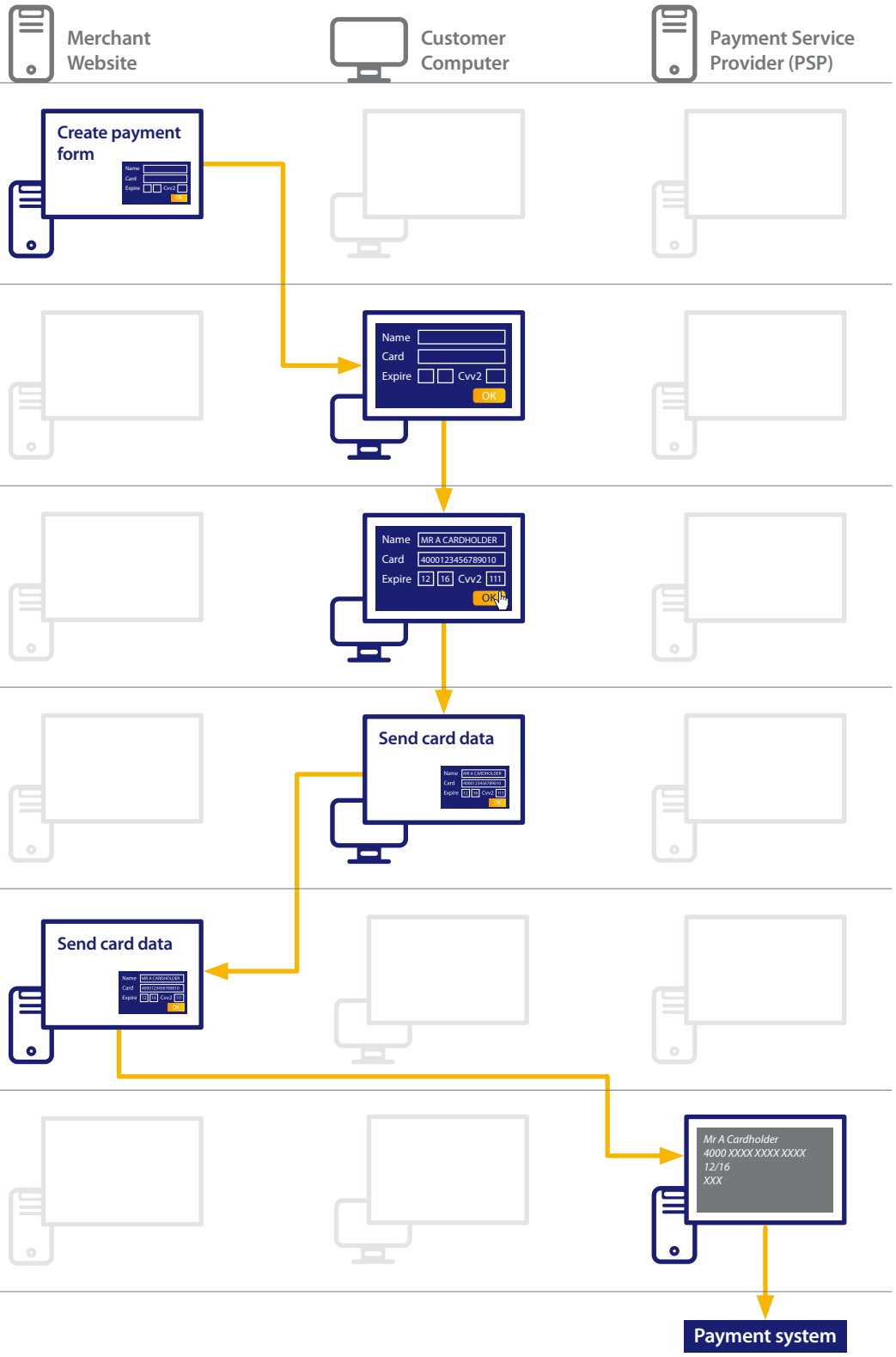
What level of PCI DSS compliance is required for the e-commerce channel?				
Merchant	Level 1	Level 2	Level 3	Level 4
	RoC[A-EP]	SAQ A-EP	SAQ A-EP	SAQ A-EP
PSP	A Visa Europe listed validated PCI DSS compliant service provider.			

Risk rating
Medium – this method of processing e-commerce payments is currently being attacked by criminals.

The API

(this is sometimes also called a 'merchant gateway' typically sending data from the merchant to the PSP formatted as XML, JSON or name:value pairs)

When the customer wants to check out:



The API

(this is sometimes also called a 'merchant gateway' typically sending data from the merchant to the PSP formatted as XML, JSON or name:value pairs)

When criminals attack the direct XML	
How	Criminals break the security of the merchant website and they change the program which receives the card data from the payment form so that the card data is also stored on the hard disk of the merchant website. Criminals then return to the merchant website to download the card data.
What will the customer see?	The payment form, the customer will not notice any difference.
What will the merchant see?	The merchant will not see any effects of this attack in their day-to-day operations but an examination of the web server will normally show the attack by the criminals.
How can the merchant detect this attack?	Requirements 10 and 11 in PCI DSS are designed to detect criminals attempting to break into and alter a system.

What level of PCI DSS compliance is required for the e-commerce channel?				
Merchant	Level 1	Level 2	Level 3	Level 4
	RoC	SAQ D	SAQ D	SAQ D
PSP	A Visa Europe listed validated PCI DSS compliant service provider.			

Risk rating
High – criminals are very likely to attack merchant websites that process cardholder data. Most data compromises occur in merchants that use this type of process.

0714-BDG-BBX-0137