It’s time to simplify the card payment process! Take the first step by ditching the three-digit CVV code, says Encoded

Submitted by: PR Artistry Limited
Wednesday, 18 May 2016

Rob Crutchington, Director at Encoded takes a closer look at the three digits on the back of a card and dispels two common myths around the card verification value (CVV) code

Paying for goods and services with a debit or credit card is now so commonplace that those wielding a fist full of bank notes are often regarded with suspicion. Card payments make life easy but the process behind making them happen is a lot more complex than you might think, with verification taking place every step of the way. We’re all familiar with giving our card details by telephone or entering them online but what happens next? There are 14 steps in card authorisation and settlement*, involving merchants, payment service providers, payment gateways, the merchant’s bank, card schemes and finally the customer’s own bank and this whole process can take a minimum one day and often far longer.

Authorisation is essential but how much information is really necessary?
For those paying online or over the telephone there is often one more step required in the authorisation process. They are asked for the card verification value (CVV) code or three-digit number on the back of their MasterCard or Visa card (four-digits if paying by Amex). The rationale behind the CVV code is that it is further validation that the customer physically has the card in their presence. But is this true and is it absolutely necessary?

Time to dispel the myths around CVV codes
There are several rumours in the industry which relate to why merchants seem to think the CVV code is necessary. One thing is for sure it cannot be retained once a transaction has been processed. Keeping it would contravene the very foundation of the Payment Card Industry Data Security Standard (PCI DSS) which prohibits the storage, hand-written or in computer files, of a customer’s confidential card data.
The two most common myths around CVV codes are:

Myth One: Merchants benefit from reduced interchange fees by using CVV codes in transactions
Many merchants believe that by insisting on CVV codes, they can benefit from a reduced interchange fee based on the transaction being deemed “secure”. The interchange fee is the
amount charged by Card Schemes such as VISA to the acquirer for using their services. However, as of the 1st of March 2015 VISA capped the rate at 0.2% for debit card transactions and 0.3% for credit card transactions across the EU irrespective of whether the transaction included the CVV or not. All mail order telephone order (MOTO) transactions are deemed as non-secure.

Therefore, it is not true that there is any financial benefit from requesting the CVV and given the huge importance PCI DSS places on the CVV, Encoded’s advice is to simply not request it in the first place.
What is true is that by including the CVV code should a dispute or chargeback occur, when a merchant submits a transaction for authorisation, the processor and/or card brands will reduce their fees on the dispute or chargeback. However this small business cost is dwarfed by the PCI DSS costs of protecting it, if accepted.
Myth Two: Merchants conducting repeat transactions need to submit the CVV for the original and all subsequent transactions

Again, this is a myth. There are two ways to conduct such recurring transactions. The easiest way is to use a payment service provider that supplies a reference number from the original transaction and then processes all subsequent transactions using the same number or token. The other option is for an organisation to store the cardholder's name, account number and expiration date, providing, of course, these details are stored securely either by encrypting them if on a computer, or if using a manual system they are physically secure.

Is it time to ditch CVV codes?
Interestingly, in a country that is often at the forefront of data protection and security, the United State of America does not use CVV codes and we should follow suit. Until recently VISA Europe and VISA Inc. were two separate organisations. However in November 2015 VISA Inc. bought VISA Europe for $23.4bn. As such we can all expect changes in the European payments market to follow the US way of handling card details. In actual fact all that is really required is the 16-digit card number and this can be stored provided it is encrypted and "deemed" unreadable as per sections 3.3 and 3.4 of v3.1 the PCI DSS requirements.

This latest development is good news because, from a PCI DSS compliance perspective, storing cards and making use of automated recurring payments will be much easier. Eliminating the need to provide CVV codes and partnering with a technology provider which has invested in the top level of PCI DSS compliance and tokenisation technology will go a long way towards simplifying the payment process for customers and protecting them against major security threats such as fraud and cybercrime. There really is no time to lose to get the right levels of security in place while ditching the three-digit CVV code.

*https://www.encoded.co.uk/day-life-contact-centre-card-payment/

805 words

-ENDS-

About Encoded

Encoded is a UK company founded in 2001 to offer affordable, pay-as-you-go IVR and payment solutions to small and large businesses. Hundreds of contact centres now rely on Encoded secure automated payments for their PCI DSS compliance requirements. Today the company's software supports many of the UK's leading brands including Virgin Holidays, Mercedes-Benz Finance and Hartlepool Water
Solutions include:

- Virtual Terminal Payments
- IVR Phone Payments
- Agent Assisted Card Payments
- Web Payments
- Automated Recurring Payments

For more information please visit ENCODED (http://www.encoded.co.uk)

Press contacts:
Mary Phillips/Andreina West
PR Artistry Limited
T: 01491 639500
E: mary@pra-ltd.co.uk