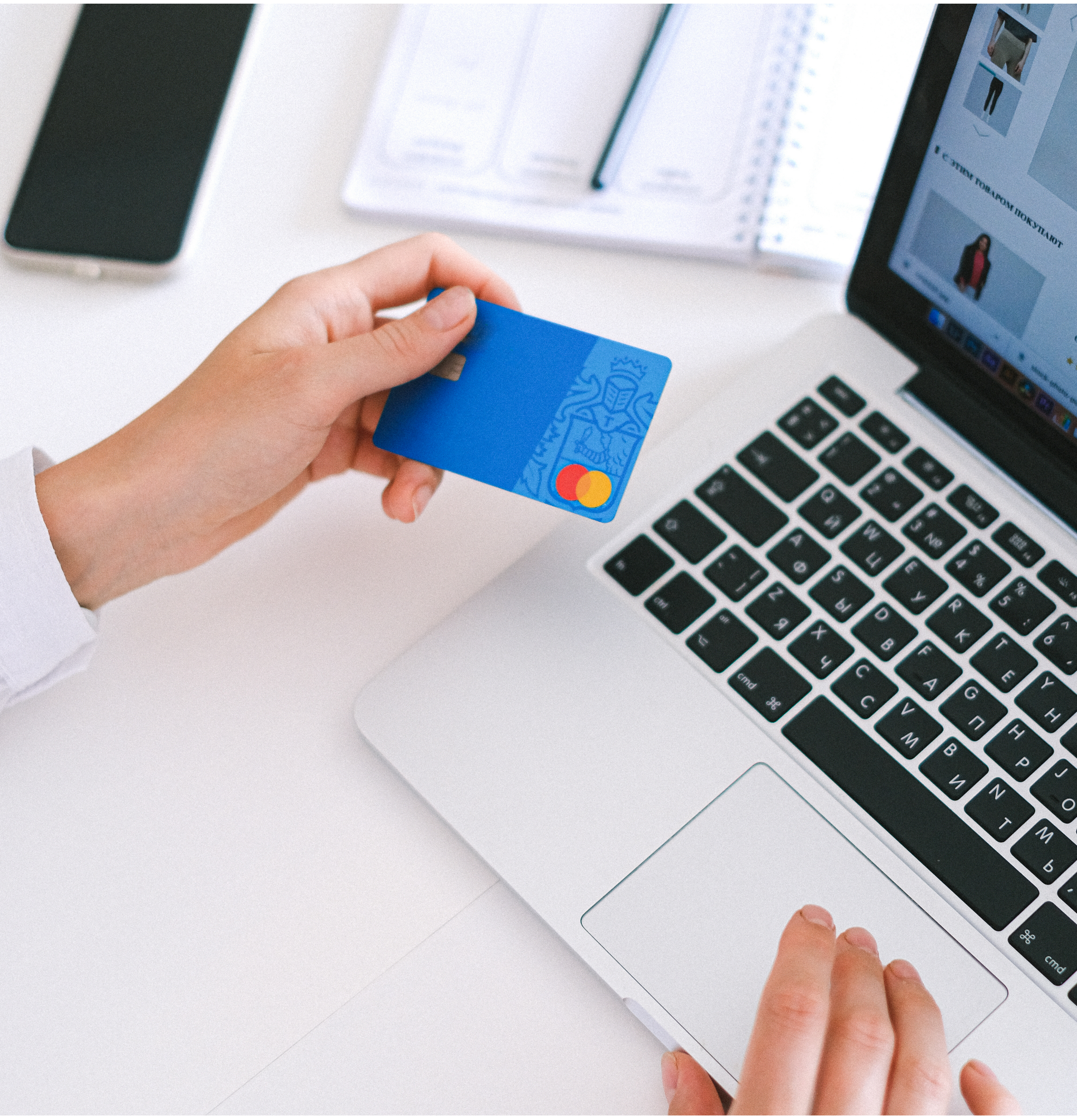
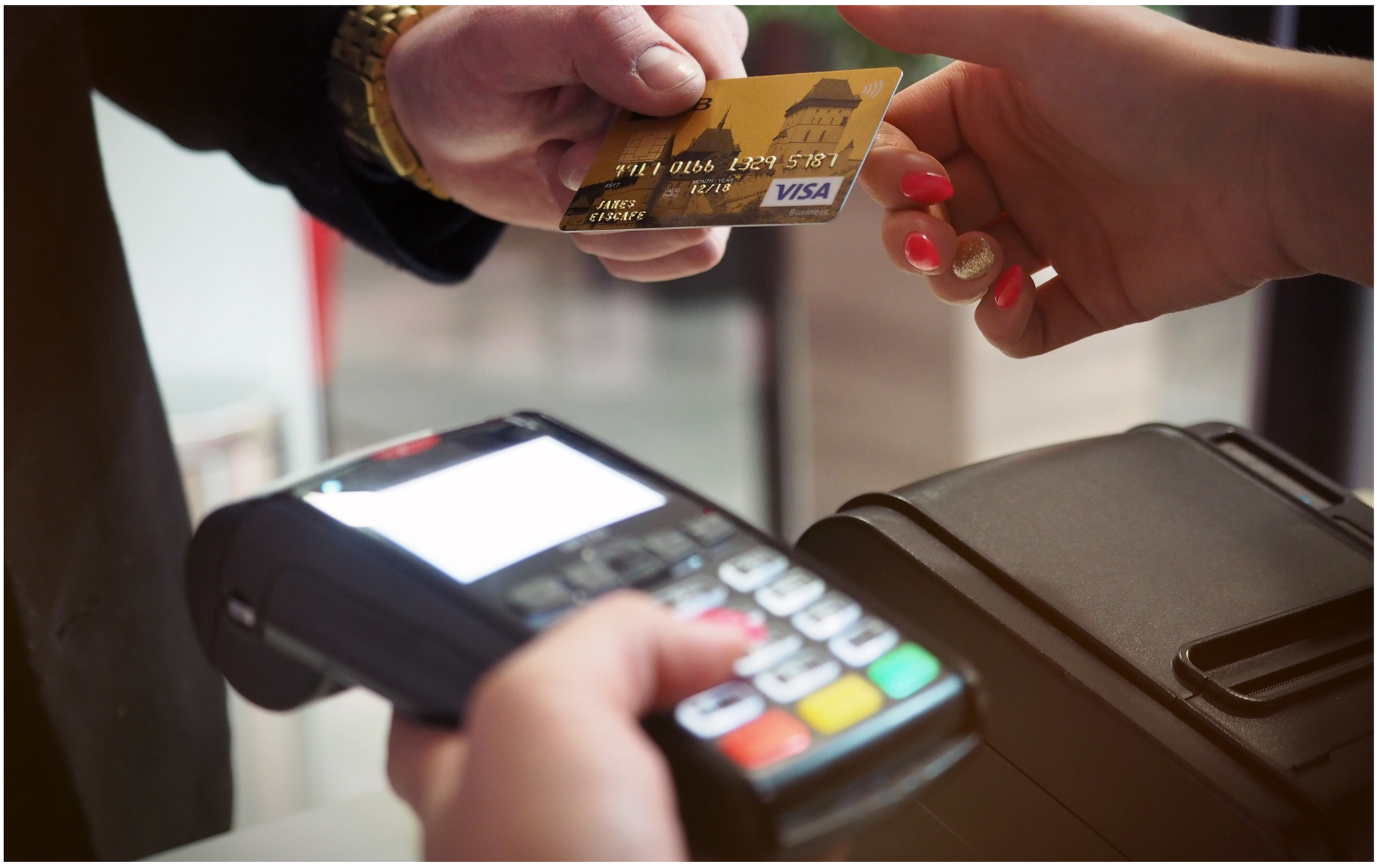
Credit Card Compliance & PCI DSS

For the Small-Medium Business Merchant





INTRODUCTION

Protecting Your Small-Medium Business From Data Breaches

The global payment ecosystem is growing, becoming more complex and is inherent with cyber risks.

In today's digital world, merchants in the ecommerce, retail, hospitality, and restaurant industries need to accept payment transactions via credit and debit cards from their customers. Because of the digitized processing of payment transactions, the credit card industry has been a target of data breaches which has a huge impact on their bottom line. So the payment card industry developed cyber security standards for all merchants, from large to small businesses, and rolled out the PCI DSS requirements.

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that ALL companies that process, store or transmit credit card information maintain a secure environment. The PCI DSS is administered and managed by the PCI Security Standards Council, an independent organization that was created by the major payment card brands including Visa, MasterCard, American Express, Discover and JCB.

CLARUS

Why PCI DSS?

With the evolution of payment cards and ecommerce, payment fraud began to rise dramatically. Hackers began taking advantage of poorly protected systems to steal customer's payment data, making merchants an easy target. As the credit card companies faced major losses, they responded to this crisis by collaborating to create the PCI Security Standards Council and all merchants, service providers, and payment processing organizations, from large to small, are now required to comply with these standards.

Who Needs to Comply?

If you are a merchant taking credit card payments through any channel, whether at the point of sale (POS), over the phone, or through ecommerce, then you are required to comply with PCI DSS. And it is your responsibility, not your merchant service provider (MSP), to be compliant.

The payment card industry (PCI) uses merchant levels, Level 1 – 4, to determine the risks and appropriate level of security required. Each level is based on the number of transactions processed per year by the merchant and also dictates the validation and testing required by the merchant.

CLARUS

Who Needs to Comply?

PCI DSS Merchant Levels		
Level	**Criteria**	**Validation**
1	Any merchant- regardless of acceptance channel - processing over 6,000,000 Visa/Mastercard transactions per year, has suffered from a data compromise, or identified by another payment card brand as a Level 1	Annual on-site security audit - and - Quarterly Network Scan
2	Any merchant processing 1,000,000 to 6,000,000 Visa/Mastercard transactions per year	Annual self-assessment questionnaire - and - Quarterly network scan
3	Any e-commerce merchant processing 20,000 but less than 1,000,000 Visa/Mastercard transactions per year	Annual self-assessment questionnaire - and - Quarterly network scan
4	Any merchant processing less than 20,000 e-commerce transactions per year and all other merchants processing up to 1,000,000 transactions per year, regardless of acceptance channel	Annual self-assessment questionnaire - and - Quarterly network scan reccomended

PCI Noncompliance is Expensive

It is mission critical for organizations to protect the data of their customers, employees, third parties and everyone else related to their ecosystem. The purpose of PCI DSS is to protect credit card and personal data.

The business risks and ultimate costs of noncompliance can greatly exceed the costs involved in complying with PCI DSS. Merchants can be charged monthly non-compliance fees, face non-compliance fines of between $5000 – $500,000, be required to conduct expensive cyber forensic investigations, risk losing data and their reputation if hacked, and/or face lawsuits.

Cyber security can be expensive, especially for a small mom-and-pop business. However, all merchants are required to comply with the PCI DSS and it is more costly if not compliant or, worse yet, are hacked.

Implementing PCI DSS should be part of a sound, basic cybersecurity strategy, which requires making this action part of your ongoing business plan and budget

CLARUS

CLARUS

About Clarus Tech Partners

Clarus Tech Partners has extensive experience in cybersecurity, data compliance regulations, and government contracting for small to medium businesses. We have expertise in technology, data protection, project & risk management, and privacy regulation to address your cybersecurity risks and data privacy compliance requirements in the U.S., Europe, and globally.

We provide an affordable and secure **Small-Medium Business PCI DSS Security Solution**.

Call or email Clarus Tech Partners for an initial consultation and to begin meeting PCI DSS Compliance.

Clarus Tech Partners

Phone : **646-926-3850**

Email: Info@ClarusTechPartners.com

Website: ClarusTechPartners.com