Connect Booster

How Secure Are **Online Payments?**

eBook

As the cybersecurity experts, a question many MSPs get asked is, how secure are online payments? People are increasingly leveraging the web to conduct business transactions. From the comfort of home, the office or anywhere with access to the internet, virtually anyone can open an account, order goods and services, schedule delivery, complete the payment process or apply for credit.

Researchers predict the online payment market will hit nearly $18 billion by 2027, which means those transactions are increasing at a 23.7% compound annual growth rate (CAGR). Those robust numbers symbolize strong demand for these services and a rising comfort level among the individuals and businesses that share information and complete business deals via the web.

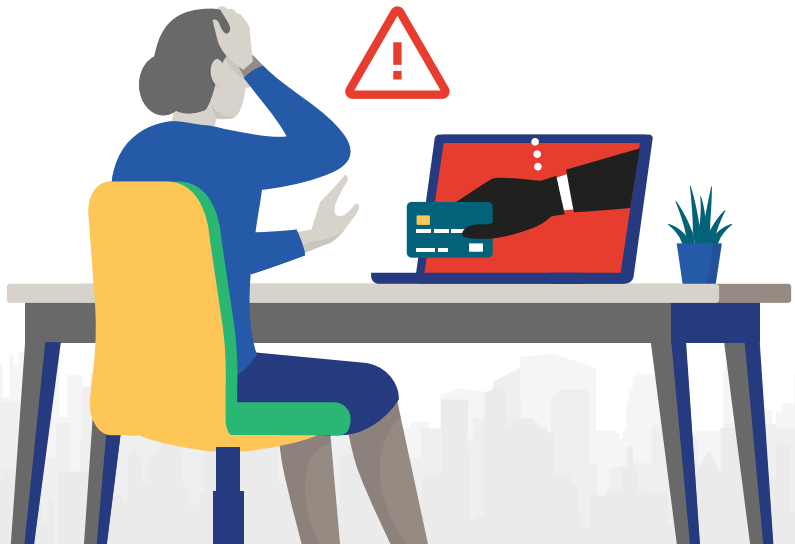
The COVID-19 pandemic helped further the case for these types of virtual payments. In March 2020, for the first time ever, the volume of transactions without a credit or debit card exceeded in-person exchanges, and that trend continues today. The web has become a commonly accepted place to conduct business transactions, and those rising numbers speak to people's confidence in the security of online payments.

Industry trends illustrate the growing trust in online transactions:

- *Researchers predict that users will spend an average of $11,755 per year on digital commerce by 2025.*
- *More than 4 in 5 (82%) people made at least one digital payment in 2021, up from 78% in 2020 and 72% five years prior.*
- *The average online transaction value is projected to exceed $1,300 by the end of 2022.*
- *More than two billion people spent $4.2 trillion globally online for goods and services in 2022.*

Technological advances, along with the growing number of online transactions and a fast-paced lifestyle, create new opportunities for cybercriminals.

Consumer preferences clearly point to online payments, but not all payment processors are created equal. As a security-conscious business that accepts online payments, are your transactions as secure as they should be? Or are you better off resorting to traditional payment methods?



Traditional payment methods are not more secure

With the proper systems in place, online payments can be more secure than traditional methods and even boost cash flow for IT services firms. Cybersecurity measures for online payments have come a long way over the past decade, with stronger industry standards and oversight as well as more advanced technologies and protocols. In many respects, these systems are more secure than onsite credit/debit card terminals and sending checks through the mail.

In-person card payments offer no assurances

Face-to-face interactions don't boost cybersecurity protection for individuals or businesses, especially when the data is collected and stored in unsecured devices and networks. Here are just a few of the many examples of data breach attacks:

- *The Target data breach exposed the data of 70 million customers*
- *Home Depot's payment terminal compromise affected 56 million cardholders*
- *The Neiman Marcus incident that impacted 3.1 million customers went on for 17 months before it was discovered*
- *180 SUPERVALU locations, including Cub Foods, Farm Fresh, Hornbacher's, Shop 'n Save and Shoppers Food & Pharmacy and liquor store locations were compromised through several attacks*

Paper checks represent a clear and present danger

Checks may be secure from digital attacks, but by using names, addresses, phone numbers and checking account details, as well as authorized signatures, criminals can make fraudulent online purchases that may not be discovered for weeks. Checks are also easy marks for counterfeiters. All they need to do is intercept a payment from incoming mail or shuffle through an accountant's inbox and jot down the key details or make a quick photocopy.

Not all online transactions are secure

Paying bills through the internet offers more assurances — when the proper protections are in place. Every business, including MSPs, VARs and other IT services providers, has a responsibility to provide its customers with a safe way to pay for goods and services online. Cybersecurity professionals have a similar obligation to ensure their clients are adopting PCI industry standards and even stronger measures to protect those transactions.

Virtually every device, application or website is vulnerable to data theft. The internet makes that easier, allowing cybercriminals to launch unrelenting attacks on multiple targets in hopes of finding a vulnerability.

Those threats are real and rising. Providing the highest level of security with encryption, tokenization and various layers of fraud prevention tools should be a priority for every IT services firm. Getting your clients to adopt the same measures is just as important. Offering that type of advice and support also creates a competitive advantage in today's high-threat and fast-paced business environment.

Adopt stronger security measures for online payments

Sharing information in a PCI-compliant environment minimizes cybersecurity risks for both buyers and sellers. The PCI Security Standards Council provides a list of minimum requirements to protect the financial security of the people who use payment card information (credit and debit cards) for in-person and online transactions.

Any business that transmits, stores, handles or accepts credit or debit card data — regardless of size or dollar amount processed — must comply. The PCI Security Standards Council also provides "quick steps to security" to ensure businesses are taking the appropriate steps to protect the safety of their customers' data. Those suggestions include:

- *Buy and use only approved PIN entry devices at your point-of-sale (POS).*
- *Buy and use only validated payment software at your POS or website shopping cart.*
- *Do not store any sensitive cardholder data on computers or paper.*
- *Make sure your wireless router is password-protected and uses encryption.*
- *Regularly check PIN entry devices and PCs to ensure no one has installed rogue software or "skimming" devices.*

One important thing to remember is PCI compliance does not ensure a company is 100% protected from cyberattacks and breaches. There are no guarantees, but following these prescribed standards helps reduce vulnerabilities and mitigate risk.

Technology to the rescue

Many businesses view payment gateways and credit card processing as a commodity, but those who select these platforms based solely on price must reevaluate their options. Not all platforms adhere to the same security protocols. Cybersecurity protections must be a priority to minimize fraud, reduce liabilities and avoid the embarrassment of a data breach. Secure payment gateways, such as the one built into ConnectBooster, offer tremendous business value and provide owners additional peace of mind.

A well-protected system captures and encrypts sensitive credit card details from a customer and transmits that data to a payment processor to complete each transaction. To optimize risk reduction, ITSPs and their customers should use a payment gateway with the following security features, such as those found with ConnectBooster:

- ***Fraud Prevention***

These measures notify businesses about suspicious transactions, such as card-spinning attacks. For example, the system may interrupt payment processing if the activity triggers one or more rules within the software. While fraud prevention cannot prevent card-spinning attacks, this feature helps businesses detect and stop attacks faster (for example, after 25 card-spinning transactions instead of 5,000), which can minimize financial losses.

Other fraud prevention measures may include the ability to:

- *Enforce a minimum/maximum transaction amount*
- *Cancel or approve any transactions flagged as suspicious*
- *Block or whitelist IPs, email addresses, countries, credit card numbers and more*
- *Establish daily, weekly or monthly limits, such as restricting a consumer from changing their credit card number more than a certain number of times during a specific time range*

- ***Point-to-Point (P2P) Encryption***

This feature protects payment card data from the payment terminal until it reaches a secure decryption endpoint. While in transit or storage, that information will be useless to cybercriminals and other unauthorized parties, removing their key incentive for payment card theft.

- ***Tokenization***

Converting sensitive data, such as credit card information, into algorithmically generated tokens with no actual value also helps foil cybercriminals. Businesses can transmit these "proxy solutions" online without disclosing sensitive data, which remains securely stored in an encrypted vault. Tokenization can drastically reduce the risk and financial impact of a data breach and make it easier for companies to achieve and maintain PCI compliance.

A secure payment gateway, as found with ConnectBooster, helps MSPs comply with those industry rules and best practices and protects online transactions. Locking down payment and credit information in a secure online portal minimizes the risks for MSPs and the clients who entrust them with that data. Mandating the use of these systems — with few, if any, exceptions — will ensure greater protection and bring everyone into the 21st century. Better yet, ConnectBooster also makes your cash flow more predictable with true autopay according to variable agreements and eliminates tedious ongoing accounting tasks.

Your customers will appreciate more than the security features of ConnectBooster. They'll also enjoy the ease and convenience of a 24/7 accessible payment portal that offers line-item billing transparency. Customers input and manage their own credit, debit and ACH data and the ConnectBooster platform does the rest. Automated workflows and integrations ensure a secure exchange of information, so each transaction goes according to schedule. That means the process to get paid is effortless, and your clients continue to receive top-notch services without interruption. Providing your customers with assurances on how simple and secure online payments can be is critical to the success of these systems.

Help your customers gain peace of mind and give them the security they expect while saving time and money every month with ConnectBooster. See how ConnectBooster offers a more secure and customer-friendly way to accept payments by scheduling a demo at www.ConnectBooster.com.

ConnectBooster adheres to industry-leading security standards to protect you and your customers, including:

- ***End-to-end encryption***
- ***Fraud protection technology***
- ***Tokenization***
- ***PCI Compliance***