Sage 100 ERP | White Paper

Payment Processing Trends, Tips, and Tricks:

What You Need to Know

sage

Over the past few years, credit and debit card acceptance has come on the scene as a required payment option. Similarly, the number of customers using credit and debit cards as a form of payment has been steadily increasing. As credit and debit cards become more pervasive, there is a growing need for business operators to understand this payment option, as well as the key components of card acceptance. Understanding payment trends, tips, and tricks will ensure your business is protected and ready for where the industry is going.

Future Trend of Payment Processing

Security

While there are many trends in the credit and debit card industry, security is the trend that most businesses should put at the top of their list. Security goes beyond locking the front door at closing time. Business operators must also secure the sensitive information their customers provide when paying for their services.

Identity theft and credit card fraud are chief concerns for consumers and the credit card industry and should have great significance to the business operator. Card and identity thieves are becoming increasingly more capable.

In 2009, there was a considerable increase in businesses affected by security breaches. In response to the growing threat, major credit card brands like Visa and MasterCard have continued to increase the scope and rigor of consumer protection standards.

The Payment Card Industry Data Security Standard (PCI DSS) has been implemented in phases, with various deadlines, to control the way card data is transmitted and stored. Credit card processors had a looming deadline of July 1, 2010, to ensure their customers operated in a PCI-compliant manner.

The PCI DSS covers many aspects of storing and handling credit card data. The PCI PIN Entry Devices (PED) component is focused on the hardware used at the point of sale (POS) for capturing the four-digit PIN on a consumer's debit card. Business owners must ensure that debit card accepting devices are PCI PED compliant, or they risk fines and fees from their processors and the card brands.

While the July 1, 2010 deadline was directed at the member organizations (banks), processors enabling the acceptance of these transactions are now also expected to ensure their customers comply with these standards. Many processors are mandating that their customers undergo a PCI audit to ensure compliance and are assessing fees for those customers that do not comply.

The goal of these fees is to encourage customer compliance, which will help reduce the risk to both the merchant and the processor. A PCI audit varies in cost, based on the price negotiated by the customer or processor, but is intended to identify security concerns, including devices, software, and processes, that may expose the merchant to the risk of data theft.

Software Serves up Innovation and Risk

Another payment processing trend in the business industry is continued software innovation. For example, numerous vendors are introducing digital technology to offer dynamic menus, as well as provide assistance with labor scheduling and advanced reporting.

It is important to note that software also falls within the purview of PCI guidelines. The Payment Application Data Security Standard (PA-DSS) requires that all software handling or transmitting cardholder data be certified. Business operators must ensure that any software used, including POS devices that run on PCs, is PA-DSS certified.

Skimming Is a Security Spoiler

While hardware and software are an obvious focus for the PCI Security Standards Council, processes within an organization are also a focus, since they greatly contribute to the security of information within a business. A process-related issue with card acceptance is the act of "skimming."

Skimming is the stealing of sensitive information by employees who handle customer credit cards. The method used to steal this information can range from using a device to capture the information stored on the magnetic stripe of the card to simply writing down the card number and the cardholder name. The former can be sold to high-tech criminals who can create fraudulent credit cards; the latter can be used to facilitate identify theft or to make purchases online.

Business operators can help guard against skimming by implementing procedural changes geared at making it more difficult for an employee to record credit card data. A PCI audit can help educate business owners and managers in applying these procedures.

What Mid-Market Businesses Should Know About Accepting Credit Card Payments

In today's competitive environment, it's important that you study and try to leverage these best practices—and even those of your competitors—to fully understand how your payment system touches your customer and your back-office operations. Taking the lowest cost route could cost you business. Consider overall cost of your merchant account, not just the discount rate percentage. Using the low-cost provider comes at the expense of limited product functionality, potential security holes, and lower levels of customer service.

1. **Embrace Credit Cards for a Competitive Edge**
   Customers buy from businesses and vendors they feel comfortable with. Asking your customer not to use a credit card might cause you to lose future sales. Additionally, if you're a business-to-business (B2B) shop, being credit-card friendly can position your business as the first alternative when your competitor is out of inventory.
2. **Maximize Your Payment Acceptance and Marketing Methods**
   Offer credit card acceptance and be accessible in all the places your customers want to buy from you: over the phone, on the web, at the tradeshow, in the field, and more. Forcing your customer to call you or conduct the sale in person may limit sales opportunities. Offering credit card acceptance for customers provides immediate payment for goods or services and can serve as a "good will" tool when customers have past-due invoices.
3. **Integrate Payment Data With Your Accounting System**
   Best practice is to integrate your payment data into your accounting system. Not only can this eliminate the inaccuracy associated with time-intensive manual data entry, but it can reduce your days sales outstanding (DSO) and enhance your audit and compliance positions.
4. **Have a Mobile Payments Strategy**
   The infrastructure is there. The technology is there. Are you there? Mobile payments are more than a PDA that can process a credit card or a mobile phone that replaces a credit card; they are also about delivering information and building loyalty through an array of mobile devices that your customers use. Mobile payments extend your business's potential to your reps in the field and beyond by enabling real-time payments in virtually any environment.

5. **Choose a Technically Savvy and Financially Stable Payments Provider**
   Today, a company's largest investment is often in technology infrastructure and information security. As a result, payment systems have moved from being bank-owned to business software company-owned and -operated. Select a technically savvy and financially stable payments provider that can meet your business's unique needs in a safe and secure environment.
6. **Get PCI Compliant and Scan Your PCs**
   PCI-DSS is a requirement of all businesses that interact with credit or debit cards. PCI certification ensures that you're up to date on the latest best practices to protect your business and customers from payment fraud. And, just as you use virus software on your PC, you should use payment security software that scans your PC and alerts you to potential security leaks—breaches that have the potential to cost millions of dollars.
7. **Use a Payment Provider That Supports End-to-End Encryption Technology**
   End-to-end encryption (E2EE) starts with your payment capture devices and goes all the way to the transaction's being authorized. E2EE prevents the card account data from being stolen electronically and lessens the cost and impact for your business to become PCI-certified.

The information contained in this material represents the views of Sage on the issues discussed herein current as of the date of publication. As market conditions are always subject to change, the information contained herein shall not be interpreted as any commitment from Sage. This material is for informational purposes only and Sage makes no warranties, expressed or implied.

About Sage North America

Sage North America is part of The Sage Group plc, a leading global supplier of business management software and services. At Sage, we live and breathe business every day. We are passionate about helping our customers achieve their ambitions. Our range of business software and services is continually evolving as we innovate to answer our customers' needs. Our solutions support accounting, operations, customer relationship management, human resources, time tracking, merchant services, and the specialized needs of the construction, distribution, manufacturing, nonprofit, and real estate industries. The Sage Group plc, formed in 1981, was floated on the London Stock Exchange in 1989 and now employs 12,300 people and supports more than 6 million customers worldwide. For more information, please visit the website at www.SageNorthAmerica.com or call 866-996-7243. Follow Sage North America on Facebook at: http://www.facebook.com/SageNorthAmerica and Twitter at: http://twitter.com/#!/sagenamerica.

Sage
6561 Irvine Center Drive
Irvine, California 92618
866-530-7243
www.Sage100ERP.com