B2B Payments: Are They Secure and Efficient?

Best practices in payments processing for business-to-business transactions
Companies rely on card acceptance as a seamless, expedient cycle of payment processing and reconciliation. Whether on the buying or supplying end of a supply chain, companies need a solution that is less expensive and less time consuming than traditional paper invoicing and check processing. Since most complex organizations today rely on card acceptance for invoice payments, learning best practices for card acceptance to help reduce cost and prevent fraud can result in significant savings across your business.

Enacting best practices starts with a review of your current payments processing solution to ensure it meets your risk-management and cost-saving efforts. On the buyer’s side, a payments processing solution should guarantee control over payables, lower management costs and ensure high levels of security. On the suppliers’ end, payments should be received quickly and with detailed reporting. At minimum, features of your solution should include visibility and tracking in a PCI compliant environment and accurate capture of payment information including detailed Level 3 transaction data.

PROTECTING YOUR ASSETS, PARTNERS AND INDUSTRY POSITION

“If you accept payments via credit, debit or prepaid cards, the major card brands — like Visa®, MasterCard® and Discover® — require that you protect cardholder account data handled by you or on your behalf by a service provider,” says Larry Brennan, VP with the PCI Compliance Team at Bank of America Merchant Services. “Protecting certain elements of cardholder account data (such as truncating the card’s primary account number and deleting the expiration date on receipts) may also be required by various state laws and federal law. Additionally, various state and federal laws contain requirements to protect customer Social Security and other personal data. The bottom line? Merchants must understand what data security laws and regulations apply to them and comply.”

PCI COMPLIANCE

“The costs of a data compromise are high,” says Brennan, pointing to the potential damage to both profits and public image. “You may be subject to significant fines and losses arising from such fraud and from not properly protecting card account information. Potentially more damaging than the financial impacts, public trust and confidence in your business can be severely eroded by a data security breach.”

Perhaps the most significant industry standard to be introduced to prevent such occurrences is the Payment Card Industry Data Security Standard (often shortened to “PCI”), a set of data security requirements established by the major card organizations to protect cardholder account information. Anyone who accepts any type of payment card transactions must be compliant with the following 12 requirements at all times:

1. Build and maintain a secure network. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Maintain a vulnerability management program. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
7. Implement strong access control measures.
8. Restrict access to cardholder data by business need-to-know. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Regularly monitor and test networks. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain an information security policy for employees and contractors.

Level 1-3 merchants must then validate or prove their compliance by meeting requirements that vary by “PCI level,” which is based on annual card transaction volumes. PCI levels range from 1 to 4, representing highest to lowest annual transaction volumes. For a complete reference guide to PCI compliance, visit PCI Security Standards Council.

How can you help to prevent data compromise and ensure compliance?

– Encourage system users to change vendor-supplied passwords for all software installations.
– Do not allow your system to be accessed remotely.
– Review your antivirus software to make sure that the definitions are current.
– If your company has experienced a suspected or confirmed security breach, take prompt action.

1. Immediately contain and limit the exposure. Minimize data loss. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information.

2. Compromised entities should consult with their internal incident response team. To preserve evidence and facilitate the investigation: Immediately alert all necessary parties, which would include: your internal incident response team and information security group, Bank of America Merchant Services Initial Response Team at 1.800.228.5882, and the appropriate law enforcement agency.
As stated in a Visa® report issued on October 26, 2010, “Franchise Data Compromise Trends and Cardholder Security Best Practices,” “Fraudsters have evolved their business models and migrated between channels, products and geographies. They continue to adapt and challenge the system.” As such, it is every company’s obligation to validate the legitimacy of every supplier and customer that provides credit card information. Specific fraud prevention tools support this process.

ADDRESS VERIFICATION SERVICE (AVS)

AVS is a service that is recommended to be used on all card-not-present (keyed) credit card transactions. AVS requires the merchant to enter the zip code at the time of transaction. When that transaction is submitted for authorization, the address and zip code entered are checked against the actual billing address and zip code for the cardholder. The AVS response provided by the issuing bank either indicates it is a match, partial match, no match, or AVS not available or error. Reduce chargeback risk by contacting the cardholder immediately if the address and zip code do not match. Note that AVS does not apply to international orders, due to language differences. Verify international orders by faxing the credit card slip to the customer and having a signature faxed back to verify the order.

CVV2

Comprised of only three numerals, but a powerful barrier to fraud, the CVV2 code is located on the back of a payment card, next to the holder’s signature. For card-not-present merchants, fraudulent transactions mean extra processing time and costs, which narrow profit margins and reduce revenue. CVV2 complements your current fraud detection tools to provide a greater opportunity to control losses and operating costs. The three-digit security code lets you know that the card is present when the customer is making a purchase online or over the phone. If a person attempts to use the card number but cannot provide a three-digit security code, or if the number is returned as invalid, the transaction should be canceled. Note that for security purposes, merchants are prohibited from storing this number.

OPTIMIZING YOUR INTERCHANGE CATEGORY

Finally, the fight against fraud requires a keen understanding of the interchange program your B2B payment activities occur within. Cardholders, merchants and financial institutions participate equally in the payments system, and interchange is the transfer rate exchanged between the merchant’s and cardholder’s financial institutions each time a transaction occurs. Interchange walks a tightrope between incentives offered by cardholders’ financial institutions (which promote and issue cards to consumers) and cost to merchants’ financial institutions (which process the transactions). Consequently, interchange varies by merchant category code, amount of the sale, payment product type, processing technology the merchant uses and even by region or country.

Within this fluctuating system, you can significantly lower credit card processing fees and help reduce the risk of fraud by supplying Level 2 or Level 3 data — the ideal combination of benefits for B2B enterprises.

Standard financial information present on all credit card transactions includes an account number, expiration date and amount of sale. These items fall under the Level 1 interchange. To qualify for Visa Level 2 and Level 3, the transaction must possess the following: AVS attempt, invoice number (or merchant-defined field for purchasing cards), an authorization amount that equals the transaction amount, and settlement of the transaction within two days.

Level 2 represents sales tax paid and allows for the capture of a unique code to assist the cardholder to sort, reconcile and report transactions.

Level 3 represents line-item information similar to what you might see on a cash register receipt. This information helps companies monitor and report on detail purchase behavior and can help ensure correct item quantity, unit price, shipping cost and other item-specific details.

This information is used to create the customer’s credit card statement as it breaks down intelligence for easy reporting and accounting, and the cardholder benefits from the enhanced data flowing back to their credit card statement. Large companies can potentially save hundreds of thousands of dollars per year in interchange costs when they implement Level 3 programs enterprise-wide. How?

– Lowering risk for cross-border transactions due to a higher level of transparency
– Streamlined back-office processes through data collection and documentation
– Easier online commerce and telesales
– Customer trust as a result of accurate credit card statements


CONCLUSION

There’s more than one way to protect your assets, opportunities, relationships and industry position. First, employ technology in the form of B2B payment processing solutions designed to combine the control and security of paper-based processes with the efficiency, and lower costs of the electronic payment system. Second, demonstrate operational excellence through reinforcing your card acceptance policies with best practices that serve to promote security, and cost reduction through efficient