The Insider's Guide to eCommerce Payment:

20 Tools Successful Merchants Are Using to Unlock Hidden Profit

Power of Payment Series

Second Edition

CyberSource®
the power of payment

CyberSource Enterprise eCommerce Payment Survey

- Phone survey conducted by Quality Research Associates
- Companies selected from lists of top eCommerce websites based in North America
- 147 Key decision maker interviews completed
- 35% CyberSource customers
- Minimum annual online revenues $10 million
- Sample average $90 million with 54% of sample >$25 million annual online revenues
- Respondents' responsibility focused on eCommerce or online payment systems or operations

CyberSource 6th Annual Online Fraud Survey

- Survey conducted online by Mindwave Research
- Industry-wide sample: companies involved in e-business activities, primarily in North America
- 348 qualified completed interviews
- 50% CyberSource customers
- Respondents' responsibility focused on online payment fraud and risk management

If you have questions after reading this guide we'll be glad to answer them.
Get expert answers from CyberSource: www.cybersource.com/askaquestion

Introduction

How much can you as an online payment manager impact your organization's profits? More than you might think. A recent survey CyberSource Corporation conducted among medium and large Web merchants suggests **better management of payment and risk practices can boost online revenue and lower costs by up to 15-20%—or more.**

This guide describes 20 tools you can use to unlock hidden profits in five key areas of eCommerce payment operations. They are derived from the CyberSource Payment Survey, the CyberSource Fraud Survey, and the experiences of many successful eCommerce organizations. Some will be obvious to you, some may be new; it is likely you'll find at least a few tools that can measurably increase your revenues and/or reduce your costs. If you have questions about any of these tools we encourage you to submit them at this address: **www.cybersource.com/askaquestion**. We'll work hard to get you expert answers.

Table of Contents

Control the Cost of Accepting Common Card Payments

Background: Since general purpose credit cards like Visa, MasterCard, American Express, Discover, etc. account for up to 90% of online consumer purchases in North America, virtually every eCommerce merchant needs to support them. The major card associations and their partners have made a huge investment in both branding and systems to make these card choices de facto standards for consumers, and they are the most important first step in online payment, at least in North America. There are significant merchant fees associated with the business these cards bring, so it makes sense to actively manage those costs. Merchants often focus on getting competitive bids on card processing to minimize costs, but there are some other specific tactics that are just as important.

TOOL 1: Manage interchange costs

At a minimum, your organization must strictly follow the rules established by card associations for card-not-present (CNP) transactions. If you don't abide by association rules, your organization can be charged at the highest "standard interchange rates." Actions that ensure your company pays lower interchange rates are:

- Always run AVS (Address Verification Service). Though this may seem obvious, research shows not all merchants abide by this common-sense rule 100% of the time.
- Fill orders quickly. Though rules differ by card brand, your organization can generally achieve lower processing rates by shipping the order and requesting settlement of the credit card transaction within 2-3 days of the authorization (see your provider for specific details).
- Set proper transaction indicators to note the transaction is card-not-present and also to note the type of card-not-present transaction.
- Pass all required data for Level II and/or Level III transactions (see Tool #4 for details).

You might also be able to save money by implementing verification programs like Verified by Visa and MasterCard SecureCode. (See Tool #12.)

Payoff: You can reduce credit card transaction costs by up to 0.8% of the total value of an order.

TOOL 2: Support debit cards

Debit card usage is becoming increasingly popular among consumers. In the off-line world, debit card usage exceeded credit card usage in 2005. If you don't support debit cards online, you could be missing out on sales and the chance to process at lower rates. Note: there are two types of debit card transactions:

Card Association-branded Check Cards. (e.g. check cards bearing the Visa or MasterCard logo) These cards are processed similar to a credit card transaction (and are processed over the same credit card processing network), but may be processed at a lower interchange rate. Note that although funds are removed from your customer's account almost instantly, your account is funded in a timeframe similar to that of a credit card transaction. Due to the differences in funding, customer service, acceptance decisioning and reconciliation considerations apply. Ask your processor about best practices for your particular business.

PIN-less Debit. Merchants/businesses in select industries are able to accept "ATM" debit cards online (without a PIN) and process the transaction directly over the debit networks (STAR, PULSE, NYCE, etc.). Savings on these transactions can be 23%-65% or more as compared to a credit card transaction. If your organization is in one of the following industries, you should encourage payment via debit card: utilities, insurance, telecommunications, cable providers, financial institutions, educational institutions and government agencies. Note: PIN-less card transactions cannot be used for automatic recurring billing payments as the customer is required to authorize each payment, and approval is required by your processor before PIN-less debit can be accepted.

Payoff: Reduce card transaction costs (~ 25-100 basis points per transaction). PIN-less debit may also provide faster funds settlement (versus credit cards or standard check card transactions) depending on your banking relationship.

TOOL 3: Offer subscription/installment payments

If your product or service is expensive, one effective method of lowering purchase resistance is to break the price into a series of installments. Not only can this yield lower banking costs for you, “subscription relationships” can mean higher lifetime value per customer and a more predictable revenue stream if enough of your customers select this option.

Payoff: **Lower banking costs (the interchange benefit of installment payments for qualified merchants is approximately 42 basis points plus $0.05 per transaction). Not to mention the customers you’ll convert due to a more acceptable, graduated set of payments.**

TOOL 4: Support Level II and Level III (Corporate and Purchasing) cards

If a fair amount of your sales are to businesses, you should consider supporting corporate and purchasing cards (also known as Level II and Level III). These cards provide an additional level of data to the purchasing business, allowing them avoid the costly administrative process of creating purchase orders, while still providing the data they need to reconcile, control and track expenses for smaller ticket items (office supplies, computer supplies, repairs, books, etc.). Some businesses use these as their only means of purchasing certain products, and you’ll need to accept them to be considered. You’ll save the cost of invoicing and likely better control your DSO (Days Sales Outstanding/how fast you collect your receivables).

The difference between Level II and Level III is the amount of data that must be accepted and passed through during payment processing. Level III provides for return of item-level detail. Chart 1 provides a comparison.

Payoff: **Faster payment (compared to invoicing), lower processing costs* (no need to generate an invoice, track payments, do collections), easier control of DSO, minimizing credit risk (vs. purchase orders or invoicing for later payment), and increased reach (some businesses require purchase via these cards).**

*Note: to qualify for the lowest interchange rate you must pass all required data at the time of processing.

1

Level II	Level III
1. **Standard Transaction Detail** 2. **Tax Amount** 3. **Purchase Order Number**	1. **Standard Transaction Detail** 2. **Tax Amount** 3. **Purchase Order Number** 4. **Order Level Data** - Shipping Amount - Destination Zip - Destination Country 5. **Item Level Detail** - Product Description - Product Code - Commodity Code - Quantity - Unit of Measure - Unit Cost - Line Item Total - Discount Amount

BEST PRACTICES NOTE: AUDITING STATEMENTS

Periodically audit and reconcile the statements you receive from processors, gateways and acquirers to insure you are paying the correct fees for card services as well as identifying opportunities to minimize transaction downgrades.

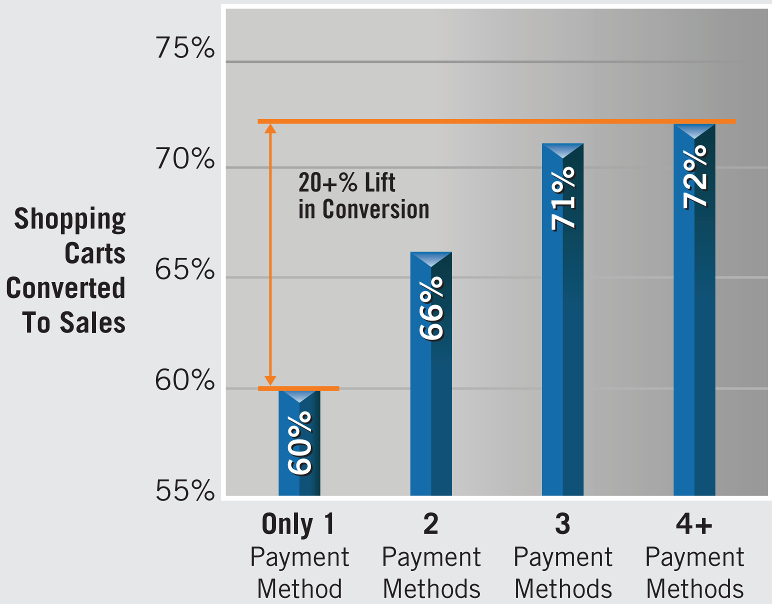
Increase Sales by Offering Additional Payment Methods

Background: According to CyberSource survey data, merchants who support payment types beyond credit cards (gift certificates, e-checks, etc.) typically see significant increases in online sales. Offering potential customers additional payment methods increases order conversion and in some cases order amounts. And this is more than just an exercise in choice. A Gallup Research survey indicates that 20% of households do not have credit cards. Certain demographic segments like teenagers do not have easy access to credit cards and 26% of potential online holiday shoppers are concerned about their credit card information being stolen (so consequently do not supply that data online). All of these people still represent a viable online customer base.

Recent research indicates that merchants who offer more payment types have lower shopping cart abandonment rates and up to 20% higher order conversion on average, as shown in Chart 2[1].

2

Offering 3+ Payment Methods Increases Sales Conversion



Payment Methods

- General Purpose / Bank Cards (Visa, MC, Amex, Discover etc.)
- Private Label Cards
- Gift Certificates/Gift Cards
- Electronic Checks
- Subscription Billing / Installment Payment
- Instant Credit ("Bill Me Later")
- PayPal or other non-card payment types

Some of the most popular additional payment types supported by successful online merchants include: Gift Certificates, Electronic Checks, Recurring or Installment billing, non-card payment types such as PayPal, and instant credit invoicing systems such as "Bill Me Later" by i4 Commerce. The options most merchants consider adding are e-checks and PayPal. Chart 3 shows the percent of merchants currently offering/planning to offer various payment options.

TOOL 5: Accept gift certificates

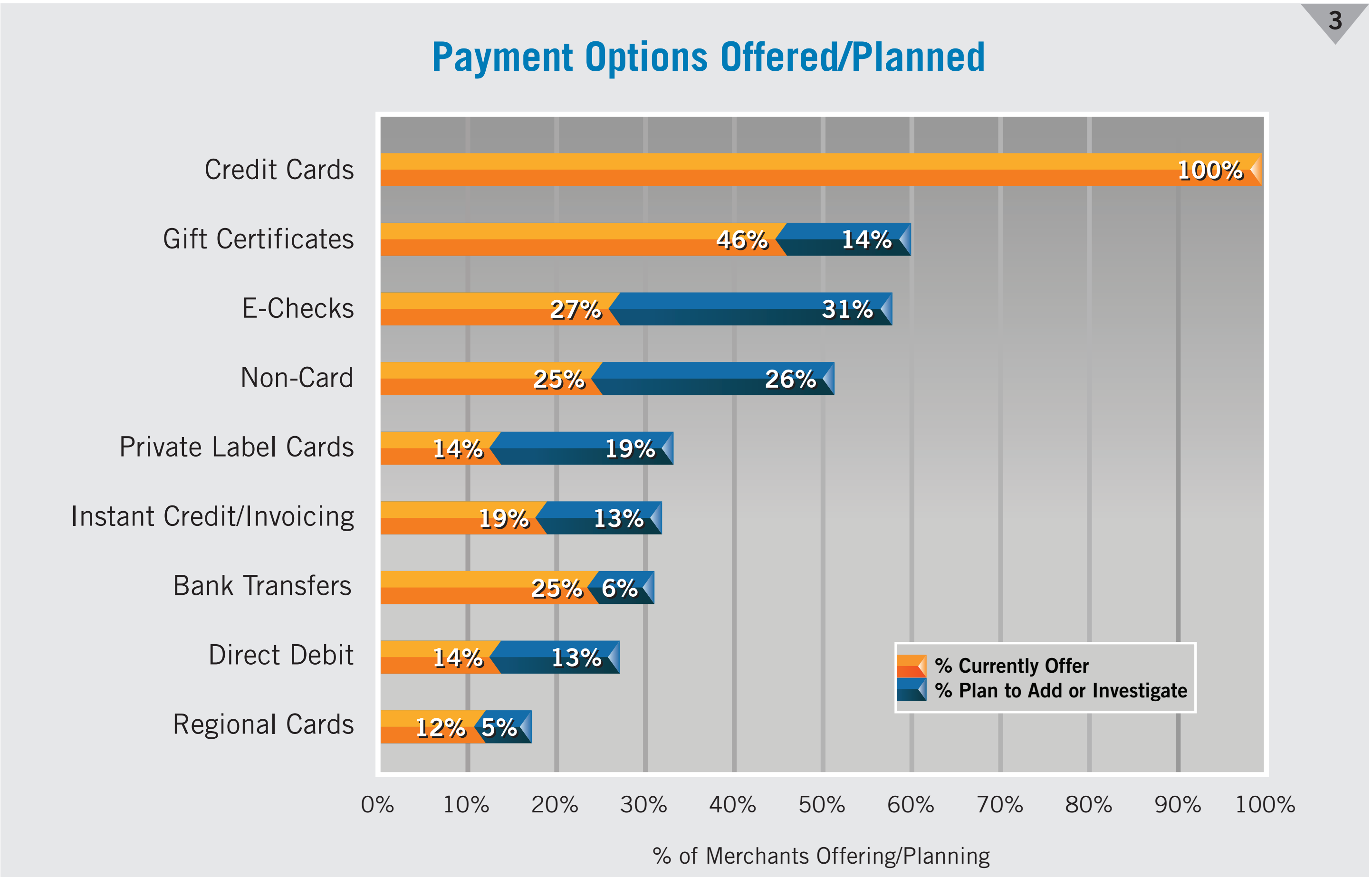
Gift cards and online gift certificates are the second most commonly accepted payment method (next to general purpose credit cards). If your organization does not currently accept this payment method you are unquestionably bypassing some revenue. Gift certificates are currently used by less than half (46%) of companies selling online, though among online retailers that number expands to 78%. This is an opportunity many companies are missing. During the holidays typically, two thirds or more of online shoppers purchase gift cards or certificates online. In the holiday 2004 season consumers planned to spend $17.3 billion on gift cards or approximately 8% of all holiday sales[2].

Payoff: **Offering and accepting gift certificates can increase online sales by 8% or more.**

[1] Order conversion metric shown is the percent of online shoppers who actually complete an online order once started, or the inverse of what is typically known as "shopping cart abandonment rate"

[2] NRF 2004 *Gift Card Survey*, November 2004

3



TOOL 6: Support electronic checks

Support for electronic checks as an online payment method is rapidly growing. Accepting checks online can expand sales by reaching out to households and shoppers who do not have credit cards or do not want to provide credit card information online. Electronic checks can include a guaranteed payment option where payment risk is passed to a third party authorizer. Also, unlike credit cards, merchants can wait for payment settlement with electronic checks before shipping goods to customers. In 2004, online electronic check volume grew by 40%, reaching 967 million transactions[3]. Major online merchants are adding electronic checks to their mix, including Walmart.com. Electronic checks are the #1 choice for the next payment method medium and large online sellers plan to add. Companies selling online who implement electronic checks typically see 3 to 8% of their sales coming through checks, with at least half of that representing sales they would have otherwise lost. Some companies have seen even larger increases[4].

Payoff: Offering electronic checks can increase sales by 3 – 8%. Depending on processing options selected, fees charged to merchants can be less than fees charged for credit cards.

[3] NACHA.org, 2004

[4] FDC/Telecheck research, 2003

TOOLS 7 & 8: Support non-card payments. Offer instant credit invoicing.

Alternative payment types such as Bill Me Later, PayPal and CheckFree are an increasingly popular payment choice among customers. Some potential buyers are averse to using credit card numbers online or simply find an account with Bill Me Later or PayPal more convenient. Invoicing and instant credit (extending credit just for the value of the purchase via real-time credit evaluation), can address potential customers who do not have credit cards, are afraid to use credit cards online, or who do not have a credit card at hand when making a last minute or impulse buy online. Services such as Bill Me Later work like a credit card (except that there is no plastic card involved), allowing the shopper to pay in full or by installments over time. One merchant experienced a 35% increase in sales after implementing Bill Me Later and average order value increased by 10%. PayPal has 78 million subscribers worldwide, and growing. In 2003 PayPal accounted for approximately 8% of online eCommerce payments and may reach 13% by year end 2005[5]. 26% of medium and large Web merchants say they would offer a non-card payment method as their next new payment offering, second in priority after electronic checks.

Payoff: Increase in sales conversion (from 8% to 30%), and new customers (up to 70% of initial Bill Me Later purchases are by customers who have never before made a purchase at that merchant site). These payment methods may, in some cases, also cost less to process.

BEST PRACTICES NOTE: ADVERTISE PAYMENT TYPES ACCEPTED

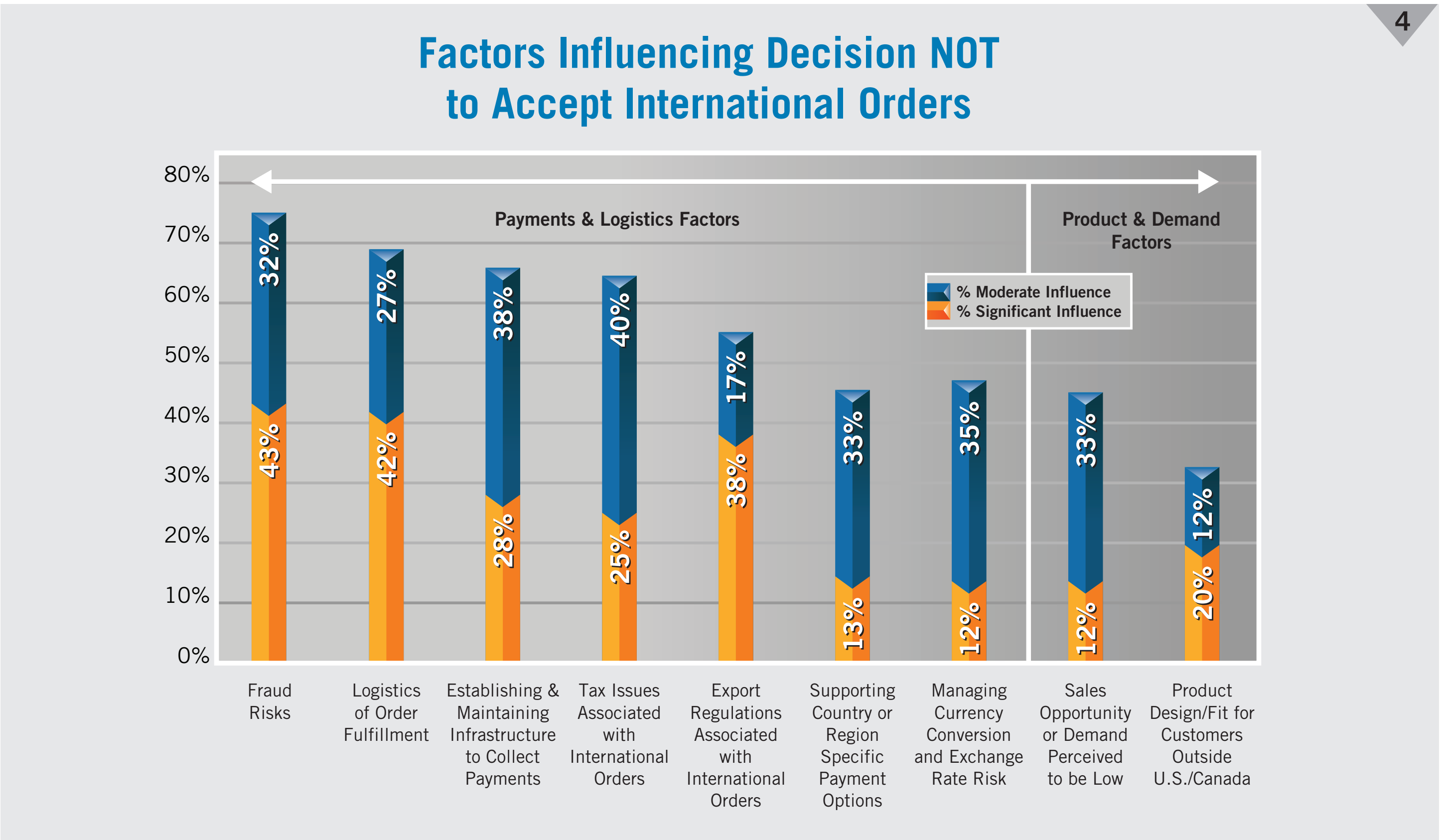
Just as brick and mortar stores advertise payment types they accept on their doors and at their checkout counters, it is important for online merchants to prominently display the payment types they accept on their website prior to checkout. By displaying the payment options available to potential customers early in the online shopping process, merchants are more likely to encourage shoppers to shop at a site and complete their purchases. In addition, catalogs that encourage people to place orders online should also include payment methods accepted by their online store.

What about global orders? How can payment management help?

Many real world factors inhibit organizations from accepting international orders—fear of fraud, challenges in order fulfillment, tax and export issues, etc. But the reality is U.S. and Canadian online merchants that do accept orders from outside North America derive between 10 and 20% of their revenues from that source. Yet 40% of medium to large Web merchants forgo that opportunity.

Why don't more companies accept global orders? The reasons cited by leading merchants are noted in Chart 4. ***Six of the seven non-product related reasons cited for not accepting global orders are payment management issues that can be effectively addressed.*** *Also, addressing global markets with locally preferred payment types can significantly increase revenues. Tactics to address payment options and banking issues are included in this section. Tactics to effectively manage fraud and compliance risks follow in the next section (CyberSource research indicates that 60% of medium and large online merchants in the U.S. and Canada successfully accept orders from outside of North America. These companies have learned how to detect and manage fraud for international orders by implementing appropriate fraud management strategies and systems).*

[5] Celent Research, 2003



TOOL 9: Enhance international sales by supporting locally preferred payment methods

The major card associations such as Visa and MasterCard have become worldwide brands. Still, many people outside of North America prefer payment methods that are more local in origin. In a fundamental way, consumer choices about money and payment reflect not just local financial systems but also local culture, such as attitudes about credit. Within Western Europe, only the U.K. and France use general purpose payment cards for more than 50% of their online purchases. In fact over 60% of EU customers overall prefer alternatives.

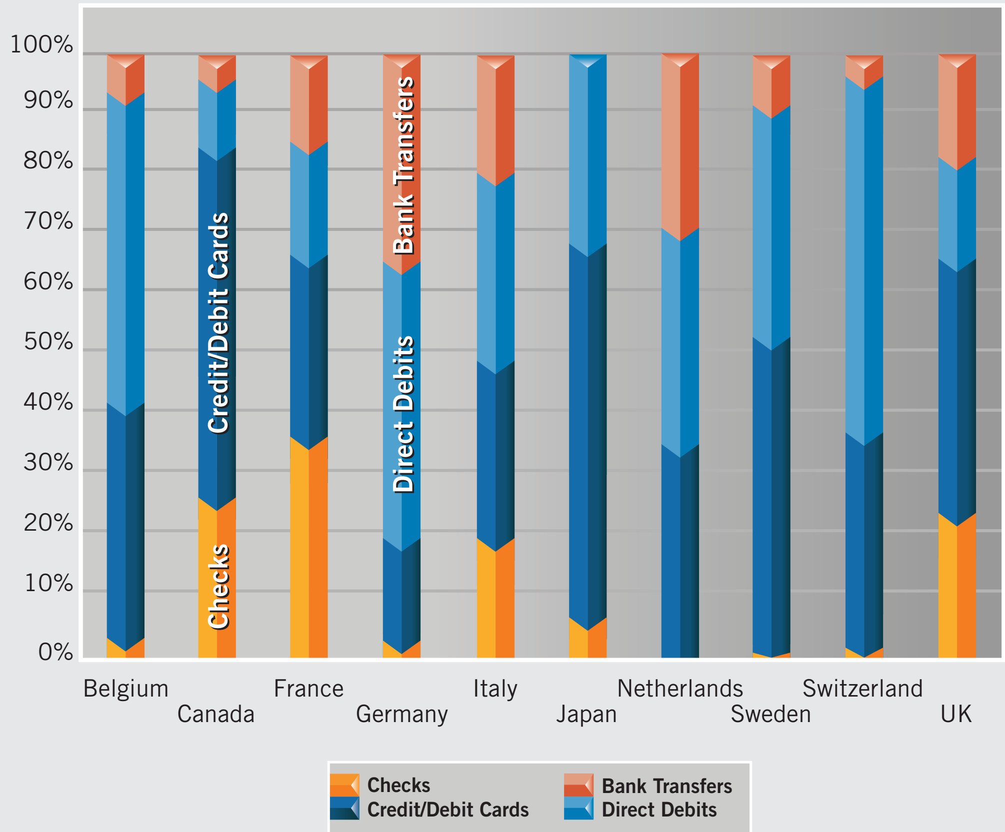
As the chart on the following page shows, other forms of payment such as direct debit bank transfers (e.g. Giros), COD or invoicing the customer directly are more popular than general purpose credit cards in some major online markets.

Despite these clear preferences, support for local country payment methods by North American companies selling online is surprisingly low. Only about 41% of global sellers support bank transfers, 23% support local country direct debit payments and 20% supported country specific credit cards. There is a real opportunity awaiting many companies here.

Payoff: Increase in sales. These increases will obviously vary widely by international product potential. One CyberSource customer estimates that by being able to accept direct debits in Germany, sales of an enterprise software product will expand 40%. Another estimates a 20% EU sales increase due to acceptance of local payment types.

5

Regional Payment Preferences



Source: Bank of International Settlements (Geneva)

BEST PRACTICES NOTE: ESTABLISH GLOBAL BANKING RELATIONSHIPS THROUGH A 3RD PARTY

Many organizations avoid global eCommerce due to concerns over the establishment of multiple banking relationships in different countries and supporting multiple local payment types. It is possible via third party payment providers to achieve this local payment capability almost instantly via one integrated payment gateway / system. There's no need to establish presence and technical connections in each country.

TOOL 10: Enhance international sales by presenting prices in local currency

Offering potential customers prices in their own, local currency can have a significant impact on sales. Dynamic currency conversion services are available now that allow merchants to present local currency prices on their site while guaranteeing the price merchants will receive in U.S. dollars or other currencies. CyberSource research indicates that of the 60% of medium and large Web merchants who accept international orders, only 30% offer prices in local currencies.

Payoff: **Can substantially increase sales in the designated currency (some merchants cite up to 400%[6]) and can hedge against changes in the exchange rate.**

[6] eCommerce-Guide.com, Christopher Saunders, "Get Paid: Making Cents of International Currency," April 15, 2004

Manage Risk and Compliance to Convert More Good Orders

Managing Risk: Background

For many merchants, the specter of fraud has had a profound impact. Although fraud rates are declining, the risk of accepting fraudulent online orders has forced most companies to manually review many online orders, increasing selling costs and risking shipment delays (see chart 6).

From 2002 to 2004 U.S. business to consumer online sales increased by 87%, an extraordinary record growth. However, the number of online orders companies manually reviewed increased 152% over the same period. On average, merchants are reviewing nearly one out of four orders received — hardly an efficient business model. To keep fraudulent credit card order rates at or below 1% (the threshold set by the card associations to avoid penalties), companies rejected 6% of all orders due to the mere suspicion that some may be fraud attempts. Over the past few years companies have been turning away an increasing percentage of online orders due to suspicion of online fraud.

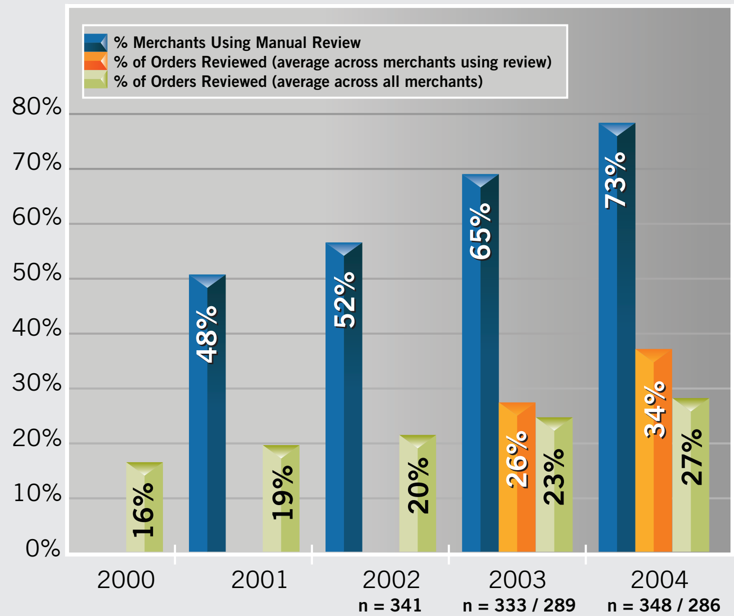
While card associations talk about relatively low fraud dispute rates for online sales, in reality they do not see the entire impact felt by online merchants trying to manage the problem. The card associations are principally concerned with confirmed fraud. Merchants handle sales that are credited without the return of the merchandise just to avoid the transaction ever reaching chargeback processing, as well as manual review and administrative costs.

Accounting for direct fraud losses, rejection of valid orders due to fear of fraud, plus manual review and administrative costs, fraud can impact up to 28% of incoming orders (actual rates vary by size of merchant).

Implementation of proper tools and processes can significantly reduce manual review costs (up to 40% or more), and actually increase sales conversion. **You can accept both domestic and international transactions while automatically controlling fraud risk.**

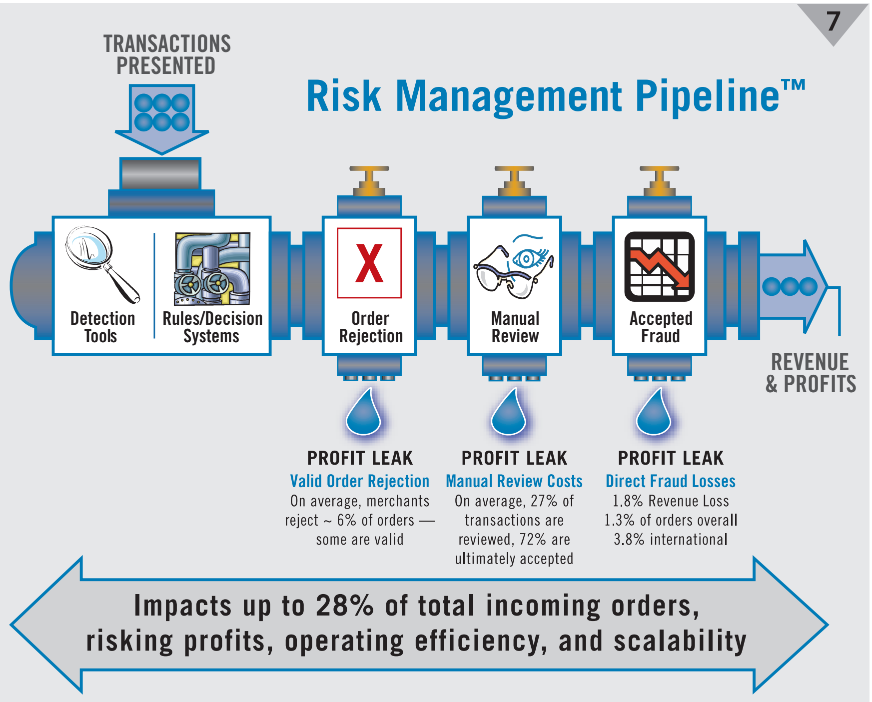
6

Use of Manual Order Review Continues to Climb



Use of manual review to manage online fraud continues to increase

7



TOOL 11: Review use of AVS and Card Verification Number (CVN)

AVS. Many merchants have automated rules to accept, reject, or review orders based on AVS (Address Verification Service) results. AVS is built-into the payment authorization process (USA and the UK). AVS only checks the numeric data in a street address and the postal code on the order and compares this with the information on record at the cardholder's bank. Responses from the processing network are numerous, but can generally be grouped as "full match", "partial match", "no match", or "unavailable" (system is down or purchaser does not reside in the USA/UK). While useful as one input to the acceptance decision, categorically rejecting or suspending orders based solely on AVS results can significantly restrict sales and needlessly increase manual order review. All response categories contain valid orders (even "No Match"). Data analyzed by CyberSource indicates merchants who accept only "Full Match" orders reject 24% of valid orders, while those accepting on "Full/Partial Match" or "Full/Partial/Unavailable" reject 16% and 1.5% of valid orders respectively. Take action to understand how much reliance you are placing on AVS results and investigate tools to complement AVS in order to optimize valid order conversion and minimize fraud risk.

Card Verification Number (aka CVN, CVC2, CVV2, CID). The card verification number is the three or four digit code printed (not embossed) on the back of most credit cards and the front of the American Express card. Validation based on this number is available at the time of payment authorization to confirm the purchaser is in possession of the card. While also not fool-proof (fraudsters can steal these numbers and publish them), requesting CVN goes a step beyond AVS in screening for fraud (with the trade-off being an extra step in the check-out/payment process which may impact sales conversion).

Payoff: **Refining how you handle AVS results and complementing AVS with CVN or other fraud tools can help boost sales up to 24% and decrease manual review.**

TOOL 12: Manage risk—implement card association payer authentication systems (Verified by Visa, MasterCard SecureCode, JCB J/Secure)

One fraud protection tool offered by the card associations involves cardholders authenticating themselves online by entering a password during the checkout process. These tools are known as cardholder authentication systems and go by brand names including Verified by Visa and MasterCard SecureCode. The card associations provide an interchange rate incentive for companies who implement and use these systems. More importantly, companies who run Verified by Visa authentication can shift the liability for fraudulent transactions back to the issuing bank. Companies implementing authentication systems find that the "liability insurance" derived from these solutions can pay for the implementation costs in just a few months of use due to lower interchange rates and shifting the cost of fraudulent charges to the issuing banks.

Note: These services have changed dramatically from their initial introduction. For instance, they now support an "in-line" authentication prompt (vs. separate pop-up-window) which better integrates with a merchant's check-out process and minimizes concerns over transaction suspension/abandonment. Lost or forgotten passwords are no longer dead ends for consumers. They are simply re-authenticated right on the spot. The impact on shopping cart conversion from implementing payer authentication systems has been reported to be minimal (typically 0.1%).

Payoff: **"Insurance" against liability for fraudulent transactions and savings on processing costs. In addition, Visa provides protection on all transactions that are checked for program enrollment, plus savings of 5-10 basis points per transaction. MasterCard extends interchange savings of 22 - 32 basis points on credit card transactions and 49 - 59 basis points on debit card transactions.**

TOOL 13: Manage risk—implement an automated decision system

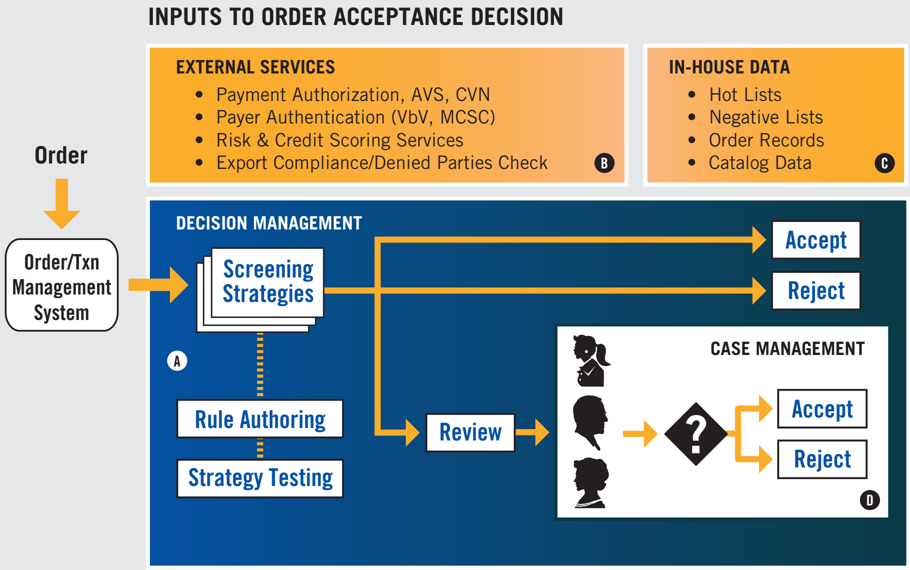
Organizations successful at managing online fraud use a variety of tools and strategies such as commercial fraud risk scoring systems, positive and negative lists, and automated decision systems using rules based on their experience. The most successful risk strategies are those that implement automated decision systems customized for a particular industry and further refined for an individual organization's specific business model. Automated decision systems provide a useful platform to integrate multiple fraud management tools and strategies aimed at reducing manual review loads and making manual review more effective and efficient. An automated decision system for managing online orders reduces the number of orders which require manual review and speeds up the manual review process by consolidating all available decision data for manual review. Some merchants have even implemented these systems under a managed services model, leveraging the fraud management expertise and resources of experienced vendors.

Decision systems automate determining whether an order should be accepted, rejected, or reviewed by providing tools for (A) Rule Authoring and Screening: business managers easily author business rules regarding order/transaction acceptance, (B) External Risk Scoring: interaction with external services that aid in automated scoring and validation, (C) Internal Tests: interaction with internal databases and systems that provide additional order/transaction intelligence, (D) Case Management: a system that holds all "suspended" transactions in a review queue (complete with all data and screening feedback) for customer service/fraud analyst review.

Payoff: **Lower manual review costs, lower IT management costs, lower order rejection /higher order conversion rates. Following are improvements CyberSource has measured where pre-installation benchmark data was available.**

8

Automating the Order Acceptance Process



Decision systems automate determining whether an order should be accepted, rejected, or reviewed by providing tools for:

- (A) Rule Authoring and Screening: business managers easily author business rules regarding order/transaction acceptance.
- (B) External Risk Scoring: interaction with external services that aid in automated scoring and validation.
- (C) Internal Tests: interaction with internal databases and systems that provide additional order/transaction intelligence.
- (D) Case Management: a system that holds all "suspended" transactions in a review queue (complete with all data and screening feedback) for customer service/fraud analyst review.

Metric	Improvement
Reduction in Manual Review	21–49%
Reduction in Fraud Rate/Chargebacks	23–93%
Increase in Automated Order Conversion	20–150%
Reduction in Order Processing Time	67%
Increase in Customer Satisfaction	43%

TOOL 14: Manage online compliance—implement real-time tax calculation

Companies that sell online need to ensure compliance with tax and other regulations in order to avoid significant penalties or negative publicity. Two areas in particular relate to payment systems and online sales—namely sales tax collection and export compliance.

There are more than 60,000 tax jurisdictions in the U.S. and Canada and approximately 100 Value Added Tax (VAT) systems worldwide. Companies with a legal nexus in a U.S. state are required to collect sales taxes for online sales made to customers residing in that state. Companies delivering more than $100,000 of online digital goods or services into the European Union are required to register and pay VAT on their EU sales.

Given the number of products taxed, different exemptions by jurisdictions and the large number of jurisdictions, tax rates are constantly changing, requiring a real-time dynamic system to correctly calculate tax liability. Shopping cart systems, where tax rates are manually entered or generic rates are applied, are likely not up to the task of correctly calculating sales taxes while minimizing tax liability.

Therefore is it worthwhile to review tax compliance with legal experts and invest in systems to calculate sales taxes correctly.

Payoff: Reduce update and maintenance costs. Avoid expensive penalties. If a company is determined to be liable for collecting sales taxes for online sales in a particular jurisdiction, back taxes may be assessed for several years (up to 8 years in some jurisdictions) and interest and penalties are likely to be assessed which can significantly increase costs by 40% or more.

TOOL 15: Manage online compliance—implement automated denied parties checks

U.S. laws prohibit sales of goods or services to certain individuals or countries. These laws now apply to domestic online sales transactions (see U.S. Patriot Act). There are multiple lists of denied parties which are continuously updated by several government agencies.

Civil and criminal penalties can be imposed for violations (see U.S. Treasury OFAC publication for more details regarding penalties and the U.S. Commerce Department Bureau of Industry & Security for export violations). The U.S. government maintains several denied parties lists with which online sellers must comply. Specific lists include:

- OFAC Specially Designated Nationals (SDN) & Blocked Persons
- OFAC Sanctioned Countries, including Major Cities & Ports
- U.S. State Department List of Foreign Terrorist Organizations
- U.S. State Department Most Wanted Terrorists
- U.S. State Department Terrorist Designation Lists
- U.S. State Department Terrorist Exclusion List
- Department of State Trade Control (DTC) Debarred Parties
- U.S. Bureau of Industry & Security - Unverified Entities List
- U.S. Bureau of Industry & Security - Denied Persons List
- U.S. Bureau of Industry & Security - Denied Entities List

Staying up-to-date with changes to these lists is possible via automated services that monitor these lists for compliance.

Payoff: Reduce update and maintenance costs. Avoid expensive penalties.

Automate Reporting and Reconciliation

Background: Internet sales are supposed to be a highly automated "hands off" 24/7 sales channel. In reality, back office processes and management tend to be manually intensive. Recurring payments, payment reconciliation, and reporting quite often involve significant manual work incurring additional avoidable costs.

TOOL 16: Optimize subscription payments

Many merchants use automated systems to avoid manual entry of subscription and installment payments. While beneficial in principle, many in-house and commercial systems aren't optimized to protect subscription revenues. Also, storage of the card or check information can present security risks.

About 1.2% of all payment authorization requests result in a "temporary payment failure." 95% of these failures can be recaptured by retrying the request during optimal capture windows. Additionally, card expiration failures can reach 2.8% per month (data on file has expired, but the cardholder and account are actually still valid). Left unmanaged, these failures place up to 20% of subscriptions at risk and increase customer service costs to follow-up when subscriptions lapse. By optimizing when retries are requested and optimizing how expired card data is handled, merchants can protect a significant amount of subscription revenues automatically—without customer service intervention.

Also, properly coding these transactions as "recurring" can also help reduce interchange fees up to 49 basis points over a standard eCommerce transaction, depending on the processor and card brand used. Merchants may also wish to consider use of a hosted service to avoid the liability associated with storing card or check information.

Payoff: Less manual intervention and cost, lower payment costs, retention of up to 20% more subscription revenues, and reduced processor authorization fees (due to selectively timing authorization retries vs. multiple-random retries which result in increased authorization fees).

TOOL 17: Automate payment reconciliation & reporting

In most companies, order systems and payment systems are not well integrated. Consequently, the process of reconciling electronic payments (i.e., the act of comparing orders transacted to payments received) is usually a manually intensive process. Manual payment reconciliation systems can negatively impact the profitability of online operations while more automated systems can contribute to profitability. It is possible to automate reconciliation and streamline administration to effectively scale with eCommerce sales.

Payoff: Automate up to 90% of manual processes and increase administrative staff productivity 30-50%. Additionally, there is potential to avoid lost revenues due to failure to identify missing payments or opportunities to recapture revenues (due to insufficient or fragmented information).

Actively Manage Payment Systems & Security

Background: Managing the systems to support multiple payment options, risk management solutions and payment administration across multiple channels is becoming increasingly complex. 50% of companies report that the complexity of managing online payment systems is greater today than two years ago, ten times the number reporting less complexity. This complexity is increasing costs and the scope of issues IT management needs to address—placing further demands on already scarce IT resources.

Payment System Management Trends

Possibly in response to this growth in complexity, merchants plan to increase adoption of outsourced/hosted payment services vs. continuing to manage all systems in-house. Currently, 34% of large merchants use a services-based model. An additional 14% of merchants plan to convert to/add a services model by 2005. If merchants carry through on these plans, use of outsourced/hosted/Web services payment solutions will reach nearly 50% by 2005. A driving factor behind this trend may be mitigating risks associated with managing payment data security.

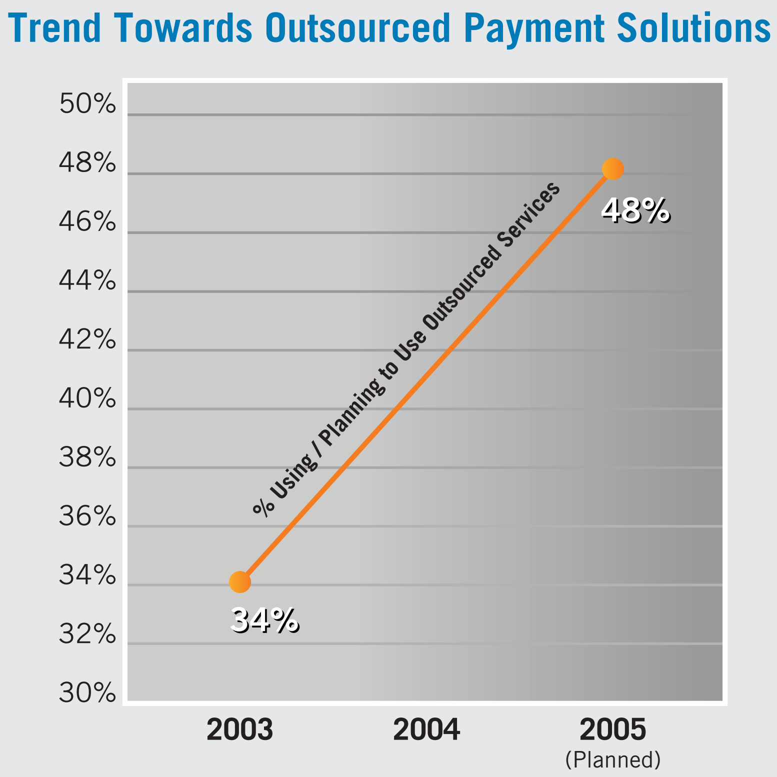
Issues IT Views as Most Critical

Among the payment system issues IT is currently addressing, Chart 10 shows issues cited as most critical.

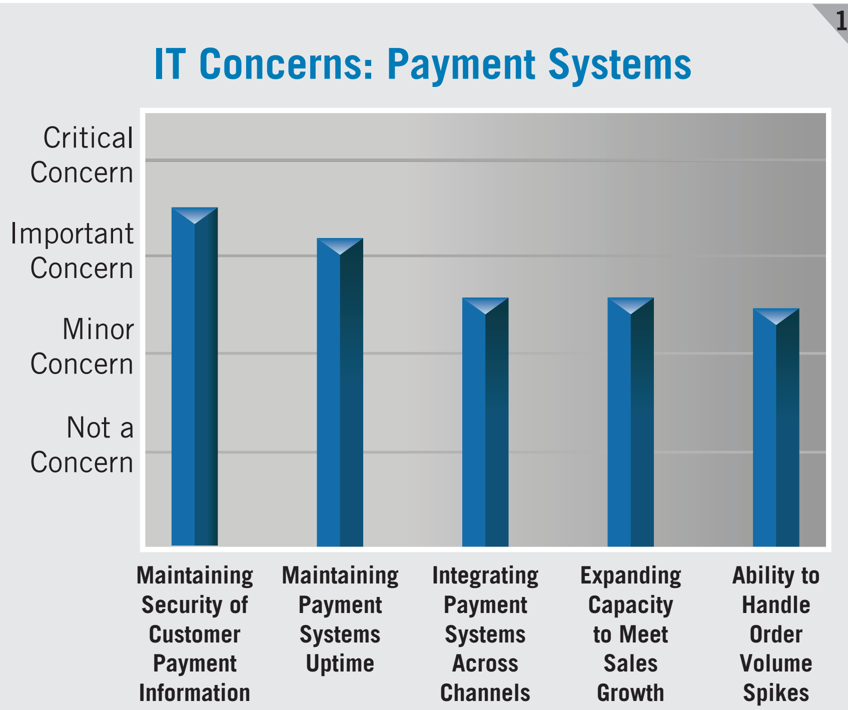
TOOL 18: Implement PCI Data Security Compliance and promote it

Despite many years of growing online sales, 69% of purchasers still express concern regarding security of payment data (during transmission or storage)[7], and this is echoed by IT management citing this as a critical concern. Articles recently reporting

9



10



[7] Ipsos-Insight Study, 2003

an upsurge of credit card data thefts at top merchants, banks and processors have only increased consumer concerns. A recent study by The Conference Board reported that 59% of online consumers say they are more concerned today about the security of their personal information on the Internet than a year ago. Some 42 percent say their level of concern has not changed; but only 4 percent say they are less concerned today. Recently the major Card Associations, Discover, and American Express agreed on a common data security standard, the “Payment Card Industry Data Security Standard” also known as PCI. Some of the PCI data security requirements are:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholderdata
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

More details about PCI standards can be found at:
http://www.usa.visa.com/business/accepting_visa/ops_risk_management/cisp_merchants.html

Failure to comply with PCI standards (independent or self-assessment audit to certify compliance and quarterly vulnerability scanning to maintain compliance) and to protect cardholder data can subject a merchant to restricted card acceptance and/or significant fines and penalties. Payment data security is a complex and dynamic problem so many merchants employ professional security experts to help with PCI compliance (full management and/or quarterly scanning management).

Payoff: **Merchants can leverage data security programs to increase consumer confidence when transacting payments online and protect brand integrity by reducing the threat of payment data theft.**

BEST PRACTICES NOTE: SECURITY & PRIVACY POLICIES

Successful merchants prominently display security and privacy policies on their sites and during the checkout process/transaction to help optimize sales results.

TOOL 19: Build for redundancy/plan for "outage processing"

Payment systems are the definition of "mission critical". If online merchants can not accept orders due to payment outages, they risk losing not just an individual transaction but the lifetime value of that customer in terms of additional orders, referrals, etc.

Build for Redundancy. To maximize uptime, top merchants seek multiple levels of redundancy in their payment systems. These may include redundancy in: processing servers, datacenters, network connectivity, processor entry points, etc. This can be achieved by building these connections directly, or by working with a service provider who maintains a thoroughly redundant architecture at all levels. Due to the large volumes processed across multiple merchants, service providers may build in a level of redundancy which would be impractical for individual merchants.

Outage Processing. Even the best designed payment system can experience temporary outages. Merchants should have an explicit plan for how orders are processed during such an outage. Merchants may have processes that "approve" the order from a customer's viewpoint (thus reducing the chance of the customer making the purchase elsewhere), and "suspend" the order for review on internal systems (having captured all order and payment information required to process). Once systems are back online, the orders can be released for processing, and any failures handled with the specific customers impacted. Of course any manual review is costly, and thus prime importance should be placed on selecting payment suppliers that deliver outstanding uptime.

Payoff: **Protects orders and preserves the lifetime value of the customer.**

TOOL 20: Investigate consolidation across sales channels

Most large merchants find they are managing a patchwork of autonomous payment systems and connections across Web, IVR, call center and other channels. This complex array of systems not only increases IT challenges, but also likely impacts administrative functions such as financial reconciliation. IP-based solutions now make it possible to service multiple channels with a single (or relatively few) payment systems.

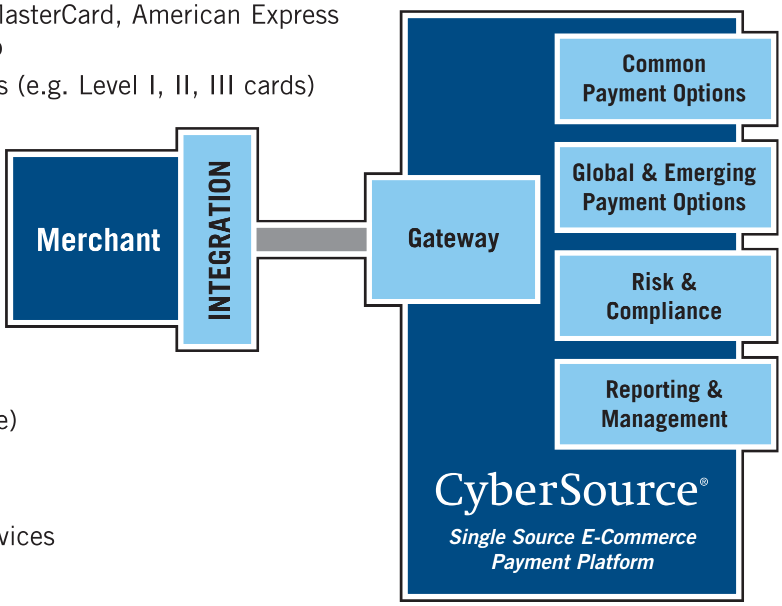
Payoff: **Merchants who are able to address consolidation across sales channels can reduce management, processing, and infrastructure costs.**

BEST PRACTICES NOTE: ENSURE "END-TO-END" INTEGRATION

One common mistake made by companies is the failure to implement "complete" payment integration—from the point of transaction acceptance through processing connections and financial systems. The ability to capture and route the full spectrum of transaction data required to qualify for the lowest processing rates, optimally screen for risk, speed review of suspended orders and streamline reconciliation demands end-to-end attention to data and systems integration. Don't look at payment as an autonomous, back-office "connection". Accepting payment is how you make money. Ensure systems are fully integrated to maximize revenues and cut costs.

About CyberSource

CyberSource offers businesses, educational institutions and government agencies a single source for electronic payment technology and related financial services. We are specialists in eCommerce with a proven record of success. CyberSource solutions are used by half of the Dow Jones Industrial companies, top Fortune 500 companies, top U.S. national retailers and major educational institutions and governmental agencies—as well as medium-sized and small businesses. We understand the business upside associated with proper payment management. We design all of our products, services and business processes to help you achieve 100% of the revenue and profit potential from your business. CyberSource solutions allow you to capture and keep more revenue, reduce the cost and complexity of payment operations, and grow without disruption. Our unique 5 point solution architecture provides you an unparalleled spectrum of global payment services—all via a single technical and business interface:



1. Support for Common Payment Options

- Processing of all major credit/debit cards – Visa, MasterCard, American Express (direct connection to save costs), JCB, Diners Club
- Consumer Cards, Corporate and Procurement Cards (e.g. Level I, II, III cards)
- Debit/PIN-less Debit
- Merchant account services
- Subscription Payments (exclusive TotalCollect™ technology)

2. Global (regional) and Emerging Payment Options

- eChecks
- PayPal, Bill Me Later
- Country-specific cards (Discover, Switch, Solo, Visa Electron, Laser, Dankort, Carta Si, Carte Bleue)
- Direct Debit
- Bank Transfers (Giro)
- Consolidated global banking/merchant account services
- Mutli-currency and dynamic currency conversion

3. Risk & Compliance Services

- Fully Managed Services
- AVS and CVN (card verification number)
- Verified by Visa and MasterCard SecureCode (payer authentication service)
- CyberSource Advanced Fraud Screen enhanced by Visa (risk scoring service)
- Decision Management Platforms – standard (hosted), advanced (hosted), custom (software)
- Global Tax Calculation (Sales, GST, PST, VAT)
- Export Compliance (export compliance and denied parties check)
- PCI scanning and professionally managed compliance services

4. Payment Reporting & Management

- Consolidated, Web-based management "dashboard"
- Transaction search and reporting in multiple formats
- Virtual Terminal for manual processing
- Automated reconciliation solution

5. Integration & Gateway Services

- Access to all services via a single interface (hosted service and software platforms)
- Flexible API (in a variety of formats, including Web Services)
- Pre-built enterprise application integrations (Cisco, Microsoft, PeopleSoft, SAP, Siebel, etc.)
- Unparalleled processing reliability & security (99.9+% uptime, PKI transaction security, certified data centers)
- Award-winning support
- Expert Professional Services

About CyberSource

CyberSource offers businesses, educational institutions and government agencies a single source for electronic payment technology and related financial services. We are specialists in eCommerce with a proven record of success. CyberSource solutions are used by half of the Dow Jones Industrial companies, top Fortune 500 companies, top US national retailers and major educational institutions and governmental agencies—as well as medium-sized and small businesses. We understand the business upside associated with proper payment management. We design all of our products, services and business processes to help you achieve 100% of the revenue and profit potential from your business. CyberSource solutions allow you to capture and keep more revenue, reduce the cost and complexity of payment operations, and grow without disruption.

Contact CyberSource to learn more about optimizing results through better payment management.

- **United States: 888.330.2300**
- **Europe: +44 (0) 118.965.3819**
- **Japan: +81.3.4363.4111**
- **Visit: www.cybersource.com**

Get expert answers from CyberSource, at www.cybersource.com/askaquestion

North America
CyberSource Corporation
1295 Charleston Road
Mountain View, CA 94043
T: 888.330.2300
T: 650.965.6000
F: 650.625.9145
Email: info@cybersource.com

Europe
CyberSource Ltd.
400 Thames Valley Park Drive
Thames Valley Park
Reading RG6 1PT
United Kingdom
T: +44 (0) 118.965.3819
F: +44 (0) 870.460.1931
Email: uk@cybersource.com

Japan
CyberSource KK
3-25-18 Shibuya, Shibuya-ku
Tokyo, 150-0002 Japan
T: +81.3.4363.4111
F: +81.3.4363.4118
Email: mail@cybersource.co.jp