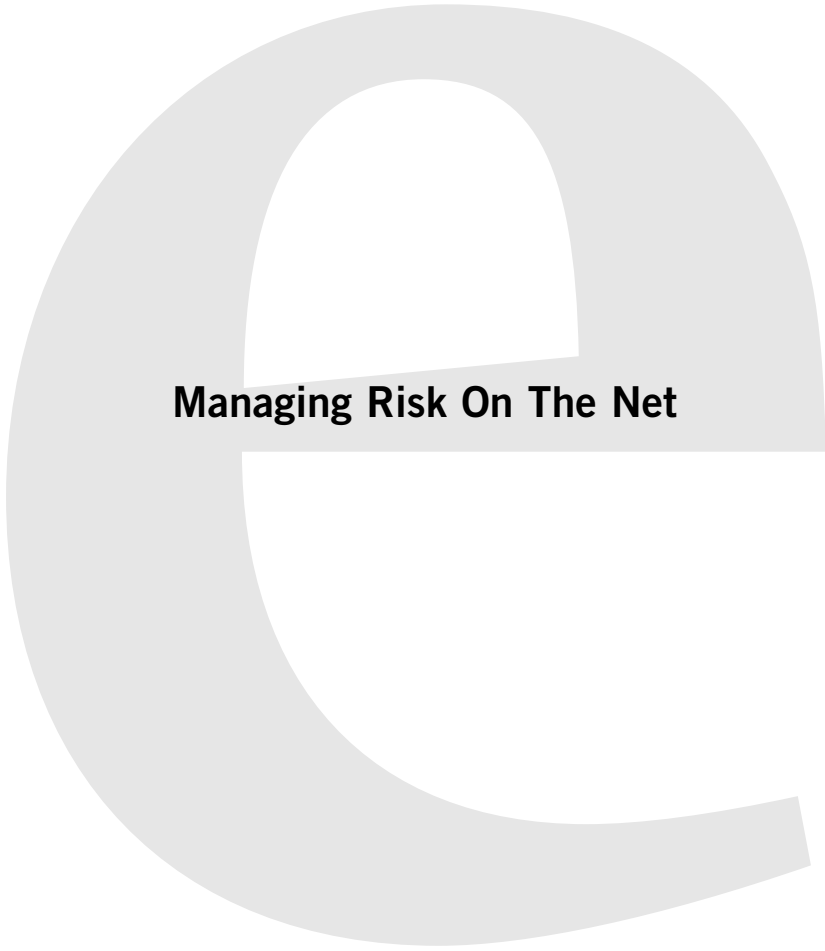


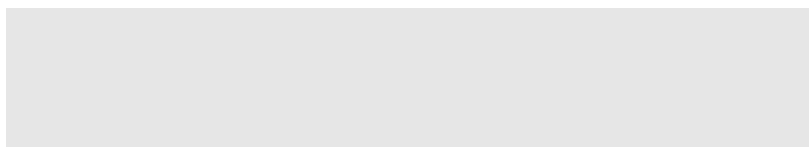
MANAGING RISK ON THE NET WHITE PAPER

What Internet Merchants Need to Know

Understand the unique characteristics of Internet fraud and the risk management strategies you can use to maximize bottom line business performance.



Managing Risk On The Net



Contents

Executive Summary	2
Understanding Internet Fraud	3
Internet Business Liability	3
Fraud Risk	3
Exception Processing Impedes Scalability	3
Why Internet Fraud Poses New Challenges	4
Identify Internet Fraud	4
Understanding the Protection Offered by Card Authorization and AVS	5
Credit Card Authorization	5
AVS (Address Verification Service)	5
CyberSource Internet Fraud Screen enhanced by Visa	6
Enhancing Bottom Line Business Performance	9
Identifying Fraud Related Costs	9
Controlling Fraud Related Expenses	9
Bottom Line Results	10
Risk Management Strategy Pro Forma	11
Conclusion	12

Executive Summary

Internet Fraud, The Same But Different

Any business that accepts bank cards accepts a certain element of fraud risk; but, as history has shown, the benefits of accepting bank cards far outweigh any of the risks. Brick and mortar businesses, as well as mail order and telephone order businesses have enjoyed years of business expansion resulting from bank card acceptance, supported by industry safeguards and services designed to contain and control the risk of fraud.

The Internet offers an equal or greater business opportunity but requires similar precautions to ensure safe business operations. The technological foundation which makes e-shopping compelling—unconstrained store access, anonymity, shopping speed, and convenience—also provides new ways for thieves to commit credit card fraud. Internet fraud is based largely on identity theft, not stolen cards. Traditional fraud detection systems were not designed for this purpose and businesses find that operating efficiencies can be impacted unless Internet-specific risk management strategies are implemented.

Unlike traditional retail transactions, Internet transactions are classified as “card not present transactions” and Internet businesses are in most cases liable for the transaction even if the transaction has been authorized by the bank. Businesses attempting to avoid fraud risk by declining all but the most ‘safe’ orders, or instituting additional manual screening methods (commonly known as “exception processing”), suffer business inefficiency and lost sales. They effectively turn away a significant portion of orders that could have been converted to sales, increase overhead costs, and limit business scalability.

Exception Processing Cripples Business

According to a study by Jupiter Communications, inefficient card authorization and fraud management strategies are the number one barrier to transaction scaling. Nearly half of all businesses surveyed reported that 11% to 75% of their orders require human intervention. Thus, “exception processing” is the number one barrier to the efficient scalability of Internet business operations.

Therefore both fraud and exception processing have a significantly negative impact on business operations. Businesses are advised to take proactive measures that streamline order operations and minimize potential risk with Internet-proven systems—just as brick-and-mortar and mail order/telephone order businesses have used methods tailored for those environments in the past.

Enhancing Operations With Internet-Purposed Systems

By augmenting traditional card authorization systems with Internet-specific screening systems, much of the risk can be eliminated automatically, thus controlling fraud risk and minimizing exception processing. Operational efficiency translates directly to the bottom line. Improvements in risk management strategies can increase net contribution by as much as three percentage points or more.

CyberSource Internet Fraud Screen enhanced by Visa is a commercially proven and validated service which allows businesses to efficiently screen Internet transactions by calculating and delivering a risk score in real time. Internet Fraud Screen is the only system to

use closed-loop card association data modeling and advanced hybrid modeling to examine over 100 different factors to calculate the fraud risk in one second (average). The system supports all major card brands and has been proven to effectively minimize exception processing and fraud risk

Understanding Internet Fraud

Internet Business Liability

Fraud poses two liabilities to Internet businesses: the cost of stolen goods and cost of chargebacks.¹

Because an Internet transaction is classified by credit card associations as “Card Not Present” transaction (the same classification as a mail order/telephone order transaction), in most cases businesses are liable for fraud—even if the bank authorized the transaction. Disputed charges result in chargebacks which impact operational productivity; and, if they exceed a certain percent of sales can impact discount rates. In severe cases, merchants may be faced with closure of their merchant account and have little chance of regaining merchant status—on the Internet, this effectively shuts the business down.

Fraud Risk

The incidence of Internet credit card fraud is highly dependent on the product category, brand, visibility of the site, and whether the product is physically or digitally delivered. Industry publications have reported fraud rates ranging from less than 1% to as high as 8%, and in some cases more.

Generally, highly visible brands, consumer electronics and “digital goods” experience higher fraud rates. Products sold can be divided into two categories—those that are tangible or “physical goods” and those that are digitally delivered or “digital goods” (products such as software, music, videos, graphics, games or information that can be delivered online in real-time). Because the latter category affords cyber thieves greater anonymity, merchants selling “digital goods” are exposed to a higher level of fraud.

Exception Processing Impedes Scalability

In many cases, the actual dollar cost of lost product pales in comparison to the wear-and-tear fraud management can have on operating efficiency. Without effective automated risk management systems purposed for the Internet, a business is faced with trying to balance order acceptance policies that are “liberal” (accepting all but the most risk-evident orders to maximize sales), and those that are “conservative” (accepting only the most “risk free” orders and rejecting or manually processes all other orders to avoid fraud risk).

Because erring on the side of liberal policies exposes the business to discount rate increases and the potential to lose its ability to accept credit cards, businesses often implement conservative automated order acceptance policies. With such policies, all remaining orders must be processed in batch and screened manually. Unfortunately, because traditional systems are used to identify “good” orders, there is still often a sizeable risk of fraud (see next section). Further, these policies can negatively impact customer satisfaction, forfeit sales, increase operating costs, and limit the organization’s ability to scale.

According to Jupiter Communications (Transaction Scaling Study 12/99), site volumes are projected to increase eleven-fold between 1998 and 2003. Sadly, only 10% of the sites report they can even double transaction capacity with current operating strategies—the key inhibitor being the degree of human intervention required to process orders. Not surprisingly, the number one reason for human intervention cited by executives is credit card processing and fraud screening (exception processing). To effectively scale and maximize profits businesses must automate valid order acceptance to the greatest extent possible.

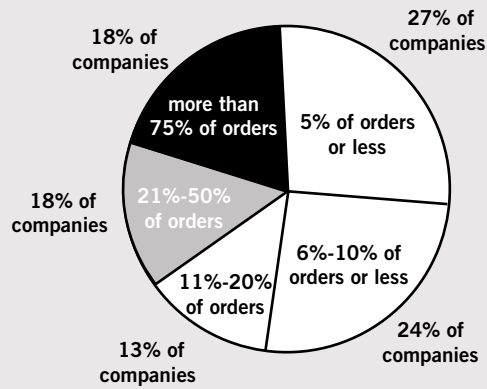
¹ A chargeback occurs when a cardholder disputes a charge, as in the case of fraudulent use of their credit card, and the bank is forced to reverse the charges.

Percent of Orders Requiring Human Intervention

Quick Facts

36% of companies surveyed require human intervention to process 21% or more of their orders.

The number one reason cited for human intervention is management of credit card authorization and fraud detection.



Transaction Scaling Study 12/99
Jupiter Communications

Why Internet Fraud Poses New Challenges

In a retail situation, the face-to-face contact and physical presence of the card helps deter theft. Embedded holograms, fine line printing, codes on the magnetic stripe, signature comparisons, and on-card photos have been deployed to effectively manage fraud and verify a card user's identity at time of card use.

Purchases made via telephone also have an element of human interaction which, although a bit more anonymous than traditional retail, still acts as a deterrent. MOTO businesses are able to match address and card number to validate identity, train operators to detect "questionable" purchases, and use the Address Verification Service (AVS). While the Internet environment is somewhat similar to the mail order/telephone order business, there are significant differences that merchants should consider.

The Internet provides a technological avenue for fraud that can be executed in ways, and at speeds, not possible in the traditional retail or MOTO merchant world. The transaction is completely anonymous, requires no human

interaction, and offers few apparent ways to verify purchaser identity (since e-mail addresses can be anonymously obtained). Fraud attempts can be initiated simultaneously across several sites, or in rapid succession at a single site.

The three prominent methods used to commit fraud against Internet merchants are:

- **Stolen Cards.** The card itself is stolen and used before the owner detects it missing; while traditional, this method is less often used to commit fraud on the Internet than others.
- **Identity Fraud.** The card itself is not stolen; thieves assume the identity of a card holder using information gained from credit card receipts, and e-mail or phone scams prompting card holders to voluntarily provide personal and bank card information. Thieves use the advantage of anonymity on the net to commit fraud.
- **Card Generators.** Fraudulent credit card numbers are generated using software programs.

In each of these cases fraud occurs because the perpetrator assumes the identity of another individual, and completes the transaction using an anonymous medium.

Identifying Internet Fraud

The anonymity offered by the Internet makes it difficult to detect fraud and to correctly accept valid orders that share characteristics with fraudulent orders. Differences in ship-to and bill-to addresses do not necessarily denote a fraudulent order, or do 'free' e-mail accounts—but they can be a clue in some cases. Consider the following. Which of these orders is good? Both? Neither? One of them? Does John really have two different e-mail accounts (maybe)? Is John really sending gifts to two different people? Maybe, maybe not. Is John really using the card, or did someone steal his identity?

Order 1	Order 2
John Smith 783 N. 43rd Street San Jose, CA 95128 surfer@flash.net	John Smith 783 N. 43rd Street San Jose, CA 95128 john@yahoo.com
Bank Card# 4784 3301 0348 1913	Bank Card# 4784 3301 0348 1913
Ship To: New York	Ship To: Texas

To efficiently manage risk, sophisticated detection systems must be implemented which augment the protection offered by traditional card authorization systems.

Understanding the Protection Offered by Card Authorization and AVS

Credit Card Authorization

Credit card authorization is the foundation of any order acceptance system and provides the fundamental information to determine whether or not funds are available for payment settlement and whether or not the card number is valid. If the card has not been reported stolen and funds are available, the transaction will be authorized. This check results in a response to the merchant: "Issuer Approved" or "Issuer Denied". This service is most often augmented by other systems when screening orders for "card not present transactions".

AVS (Address Verification Service)

AVS is currently beneficial for supporting the screening of purchases made by US consumers. The AVS check, designed to support mail order and telephone order businesses, is usually run in conjunction with the bank card authorization request. AVS performs an additional check, beyond verifying funds and credit card status, to insure that elements of the address supplied by the purchaser match those on record with the issuing bank.

The following is a summary of responses merchants can receive from an AVS check:

While most merchants will not accept orders involving issuer declines or AVS=NON-MATCH, the automated nature of an online transaction requires merchants to implement policies and processes that can handle instances where the card has been approved, but other data to validate a transaction is questionable. Such instances include cases where the response is "Issuer Approved" and AVS = PARTIAL MATCH or UNAVAILABLE (e.g., the purchaser's bank approved the transaction, but it's not clear whether the transaction is valid).

Because a significant amount of legitimate sales are associated with AVS responses representing unknown levels of risk (or purchases made outside of the United States where AVS does not apply), it is critical to find ways to maximize valid order acceptance with the lowest possible risk. Categorically denying such orders negatively impacts sales and customer satisfaction, while blind acceptance increases risk. Further, even AVS=MATCH responses carry some risk because stolen card and address information can prompt a "MATCH" response.

To address these instances, businesses have augmented card authorization and AVS results with commercial fraud screening systems.

Response	Description
AVS=MATCH	The first five digits of the street address, the zip code, and credit card number match those on record at the bank.
AVS=PARTIAL MATCH	There is a partial match (e.g., street matches but not zip code, or zip code matches but not street).
AVS=UNAVAILABLE	The system cannot provide a response. This result is returned if the system is down or the purchaser does not reside in the United States (AVS is only available for US residents).
AVS=NON-MATCH	There is no match between the data elements

CyberSource Internet Fraud Screen enhanced by Visa

A premier system specifically designed to screen for Internet fraud is CyberSource Internet Fraud Screen enhanced by Visa. Internet Fraud Screen (IFS examines Internet transactions (all major card brands) and measure the level of risk associated with each order, returning a related risk score back to the merchant in real time.

Merchant initiate a service request over the Internet using the secure messaging protocol supported by the CyberSource Commerce Component. The transaction information supplied with this request is then evaluated (using advanced “Hybrid Modeling” techniques) and compared to the merchant’s predetermined risk threshold to complete the risk assessment. Results are returned to the merchant in real time for order disposition and processing.

Closed-loop data modeling. Unlike other systems that rely on consortiums or merchants to voluntarily supply transaction results/charge-

back data (which can be inconsistent and skewed), IFS uses a unique “closed-loop” risk modeling process that is based directly on card association settlement data. The result is superlative accuracy because fraud models are built based on actual transaction results known by the card association.

IFS routinely compares each transaction to the actual transaction result that is conclusively and consistently categorized by Visa. This closed-loop process enables the service to adapt to new or changing fraud patterns and deliver highly accurate risk scores (figure 1). ‘Pure Internet’ transaction data is used to model fraud behavior (the predictors of Internet fraud are different than those used for traditional fraud detection and most be modeled based on Internet data to optimize accuracy). To ensure confidentiality and cardholder privacy Visa provides modeling results only, and does not share individual cardholder data

during model development, model enhancement, or real-time fraud screening processes.

Advanced, Hybrid Modeling. Most systems use one or two approaches, “rules-based expert system modeling” which is able to detect well understood inconsistencies in data or behavior, or “neural net modeling” which is able to identify subtle inconsistencies in data or behavior.

Neural network modeling is a technique which uses a series of sophisticated polynomial equations, each designed to detect certain fraud characteristics. It is the mathematical equivalent having a panel of fraud detection specialists, each engaged to examine the order of characteristics warrant their expertise. The individual ‘tests’ are then combined (pooled) to deliver the final ‘neural net’ score (Figure 2).

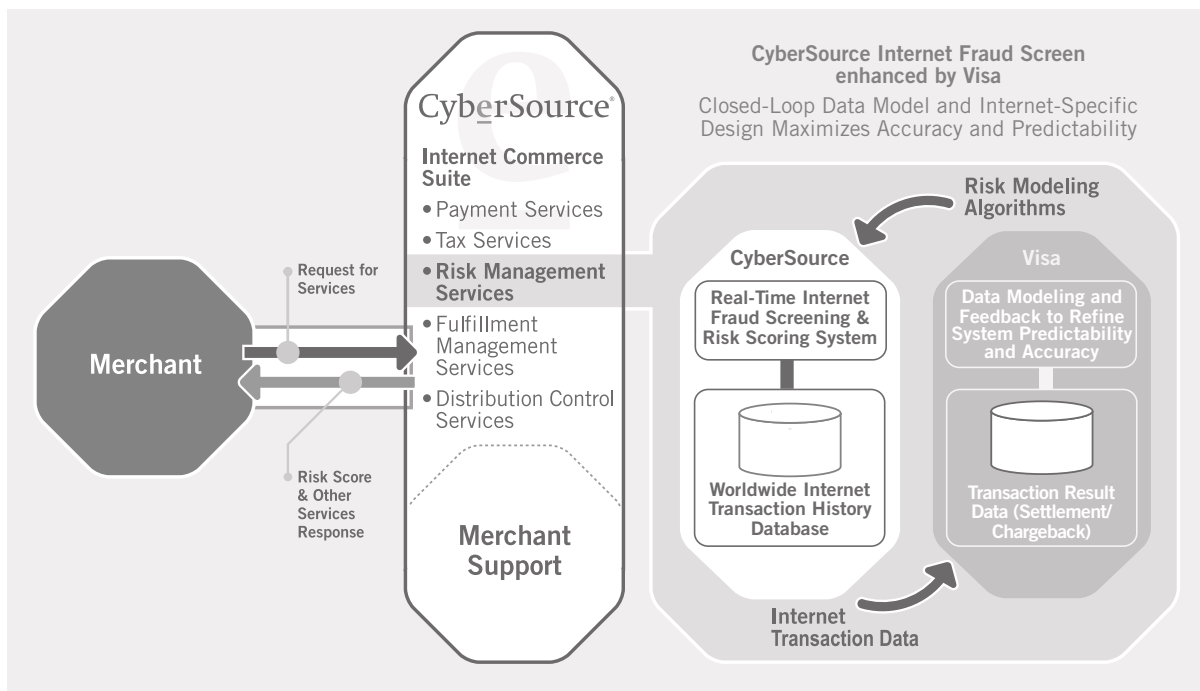


Figure 1

CyberSource Internet Fraud Screen enhanced by Visa

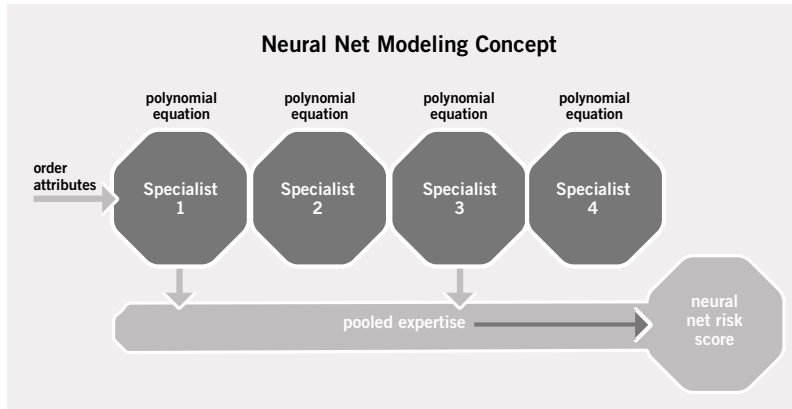


Figure 2

Experience has shown that each fraud detection method is excellent at detecting certain types of risk that the other is not. IFS combines these approaches, using “Hybrid Modeling” enhanced by Visa to examine over 100 different factors in an average time of < 1 second and deliver a single, highly accurate

risk score (Figure 3). The risk score represents the probability of fraud associated with the order on a scale of 0-99. This modeling approach results in higher fraud detection rates and lower incidence of false alarms (rejection or alerts on valid or alerts on valid orders).

Hybrid Modeling

- 1 Merchant submits order data and transaction attributes, along with risk threshold and desired factor settings.
- 2 Data is evaluated using the rules-based and a "rules-based score" is generated.
- 3 The test results data is passed to the neural network fraud model (enhanced by Visa) and a "neural net" score is generated.
- 4 The results of each test are 'blended' using sophisticated mathematical algorithms. A risk score from 0-99 is generated, representing the most accurate assessment of the risk associated with the order.
- 5 The score is compared to the merchant risk threshold and a response is returned to the merchant, including the score, all transaction data, and Risk Profile Codes.

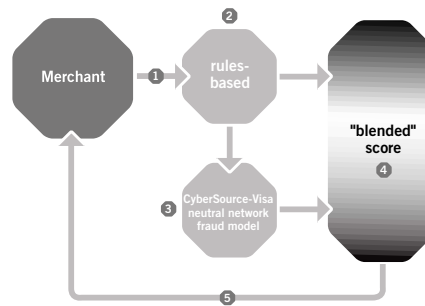


Figure 3

CyberSource Internet Fraud Screen enhanced by Visa

Code Title	Code	Description
Excessive Address Change	A	the customer has 2 or more billing address changes in the last (timeframe)
Bin Check	B	the bin check failed
High Count of Unique Credit Cards	C	the customer has more than "X" credit cards in the last (timeframe)
Domain (Host)	D	the customer has a risky domain (IP) or e-mail address
Fraud List Flag	F	a previous merchant has incurred a chargeback with no return of product
Geo-location Inconsistency	G	the correlation between the customer's e-mail or IP address (and possibly other factors) and stated billing address is suspicious
Name Change	H	the customer using this card has 2 or more name changes in the last (timeframe)
Internet Inconsistency	I	the correlation between the customer's phone number, billing address, shipping address and other factors has been determined to be suspicious
Nonsensical Input (gibberish)	N	the customer input contains highly unbelievable data in the customer name and address fields
Obscenities	O	the customer input obscene words in th order form
Time Hedge	T	the customer attempts a purchase outside the expected hours for purchase of the item
Unverifiable Address	U	the bill_to_address or ship_to_address is not verifiable
Velocity	V	this card has been more than "X" times in the last "Y" minutes
Warning	W	there is only a partial address match
Unclear Request	Z	the information in the request contains an unusual or unexpected value; examine the request carefully for abnormalities in the order
Time	displays 00:00 format, the order time in the customer's local time	
Host Severity	numeric 0-5 format; the risk associated with the customer's e-mail domain	

Figure 2

Risk Profile Codes. Risk Profile Codes identify the conditions that contribute to an overall IFS score. Codes are associated with 15 categories of tests that are included in the scoring process, as well as information regarding the customer's e-mail host (Figure 4).

Businesses are able to integrate these codes with their customer service screens, allowing customer service staff to identify the reason(s) for a high risk score. Using these codes customer service personnel can quickly act on customer inquiries or take proactive measures to convert high risk orders to low-risk sales.

Enhancing Bottom Line Business Performance

Identifying Fraud Related Costs

To assess how various risk management strategies impact net contribution, one must review how each addresses the following areas of business operations:

Ability To Prevent Loss Of Product And Associated Shipping Costs. The obvious impact of fraud is the loss of product plus the shipping and handling costs associated with the order.

Ability to Minimize Chargeback Related Costs. The most quantifiable costs are those associated with bank fees and staff time. Indirect costs include cash management problems and increases in the discount rate.

- **Bank Fees and Customer Service Staff Time.** Each chargeback results in loss of revenue and bank fee for handling the chargeback. Further, handling disputed transactions and chargebacks consumes valuable employee time. Accounting a customer service staff must engage with customers and the bank to resolve each and every chargeback.
- **Cash Management and Discount Rate.** Chargebacks can significantly impact cash flow. If businesses experience a high incidence of fraud, it is difficult to accurately assess revenues and manage accounting functions. In some cases banks will require merchants to increase reserves to cover this cost.

Too many fraudulent transactions and chargebacks result in penalties and less than favorable discount rates from the bank (typically when chargebacks reach 1% to 2% of sales).

Ability to Minimize Exception Processing.

Exception processing occurs under two conditions, 1) when valid orders are incorrectly rejected, thus requiring customer service intervention to convert the order to a sale, and 2) when automated order acceptance policies are inefficient and require customer service/risk management staff intervention to screen incoming orders prior to acceptance or rejection. Related to exception processing is the opportunity cost of rejecting or delaying processing of valid orders which are ultimately never concerted to sales.

Controlling Fraud Related Expenses

When assessing risk management strategies it is important to note that the percent of fraud captured by fraud detection systems is somewhat positively correlated to the level of fraud exposure (e.g. fraud capture rates are not static, they vary with the level of fraud exposure). Thus, modeling the level of cost control is highly dependent on the specific business environment and the fraud system used. However, some general cost profiles can be built to illustrate trade-offs.

Typically, a liberal risk management strategy based on traditional card authorization systems is least able to control costs associated with the loss of product and also results in moderate chargeback costs. This strategy is also likely to witness higher discount rates and merchant account risk.

Conversely, a conservative strategy based on traditional card authorization systems is least able to control exception processing costs—and, depending on COGS, can also be challenging to control product related expenses. Internet-specific screening systems, like CyberSource Internet Fraud Screen enhanced by Visa, are best able to control costs in all three areas of business operations (Figure 5). Results are based on the scenario modeled in the last section of this paper “Risk Management Strategy Pro Forma”.

Bottom Line Results

Risk management strategies should not be assessed simply on their ability to control fraud, but rather how well they balance costs and sales conversion to optimize net contribution. The use of an Internet-purposed risk management system, such as IFS, typically yields a significant increase in net contribution over non-Internet-purposed systems (Figure 6). Results are based on the scenario modeled in the last section of this paper “Risk Management Strategy Pro Forma”.

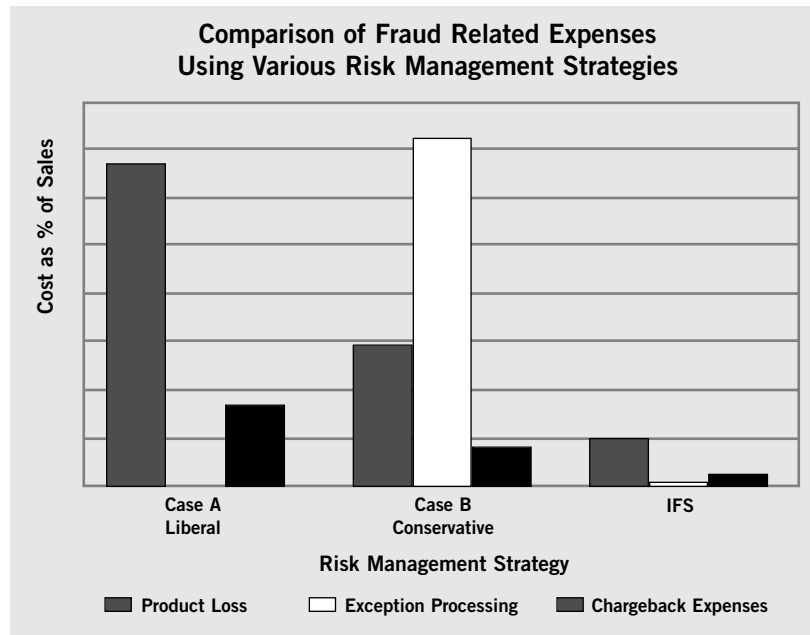


Figure 5

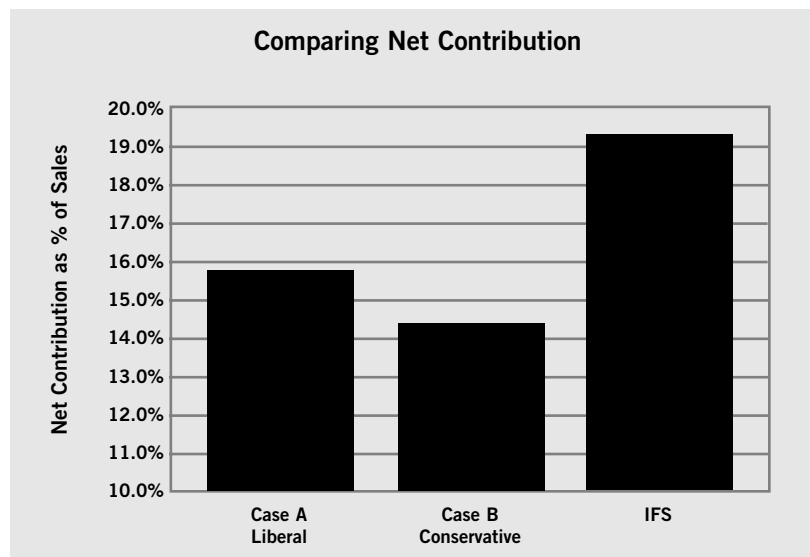


Figure 6

Enhancing Bottom Line Business Performance

Risk Management Strategy Pro Forma

The comparison below offers a framework for assessing the net contribution impact of three risk management strategies and systems. Assumptions are noted at the top, followed by the pro forma resulting from those assumptions.

Scenario Assumptions & Calculations			
	Case A Liberal ¹	Case B Conservative ²	IFS ³
Attempted Orders (000s)	1,000	1,000	1,000
Issuer Declined (no authorization received)	4%	4%	4%
AVS="No Match" (failed address check, available US only)	6%	6%	6%
Total Orders Declined or Flagged by Traditional Systems	100.0	100.0	100.0
Potential Viable Orders	900.0	900.0	900.0
Post Authorization Fraud Level	4%	4%	4%
Percent of Fraudulent Orders Not Detected ⁴	100.0%	45.0%	15.0%
Net Fraud Rate Experienced	4.0%	1.8%	0.6%
Percent of All Orders Accepted Automatically	100.0%	65.0%	100.0%
Percent of All Orders Requiring Exception Processing	0.0%	35.0%	0.5%
Percent of Valid Orders "Alerted" (rejected or flagged for manual screen)	0.0%	32.0%	0.5%
Percent of Valid Orders "Alerted" That Will Be Recovered	99%	99%	99%
Number of Orders Accepted Automatically	900.0	585.0	900.0
Number of Orders Required Exception Processing	0.0	315.0	4.3
Actual Valid Orders	864.0	864.0	864.0
Number of Orders Incorrectly Identified as High Risk	0.0	276.5	4.3
Number of Orders Not Converted (lost sales)	0.0	2.8	0.0
Valid Orders Accepted (after screening and exception processing)	864.0	861.2	864.0
Fraudulent Orders Accepted	36.0	16.2	5.4

Notes

¹ Case A (Liberal Acceptance Policies): automatically accept all orders except issuer decline and AVS = NO MATCH

² Case B (Conservative Acceptance Policies): automatically accept only issuer approved and AVS = NO MATCH

³ IFS: CyberSource Internet Fraud Screen enhanced by Visa

⁴ The PERCENT of fraud undetected by automated systems is inversely related to the magnitude of fraud experienced. (e.g. the higher the rate of fraud, the higher the PERCENTAGE of fraud captured by IFS)

Order Acceptance Criteria: Digital Products			
	Case A Liberal ¹	Case B Conservative ²	IFS ³
Sales			
Total Orders Processed (000s)	900.0	877.4	869.4
ASP	\$ 100	\$ 100	\$ 100
Gross Sales (\$000)	\$ 90,000.0	\$ 87,743.5	\$ 86,935.7
(Less Fraud)	\$ 3,600.0	\$ 1,620.0	\$ 540.0
Net Sales	\$ 86,400	\$ 86,124	\$ 86,396
COGS and Shipping Expenses (as % of sales)	80%	80%	80%
COGS and Shipping Expenses	\$ 69,120.0	\$ 68,898.8	\$ 69,116.5
Gross Margin (\$000)	\$ 17,280.0	\$ 17,224.7	\$ 17,279.1
Exception Processing and Fraud Costs			
Cost of Product Lost to Fraud	\$ 2,880.0	\$ 1,296.0	\$ 432.0
Exception Processing Cost Per Order (order review/call center time)	\$ 10.00	\$ 10.00	\$ 5.00
Exception Processing	\$ -	\$ 3,150.0	\$ 21.6
Bank Fee Per Chargeback	\$ 10.00	\$ 10.00	\$ 10.00
Administrative Cost to Handle Chargeback	\$ 10.00	\$ 10.00	\$ 10.00
Chargeback Related Costs	\$ 720.0	\$ 324.0	\$ 108.0
Discount Rate Relative to "Standard"	high	standard	standard
Total Costs Due to Fraud (\$000)	\$ 3,600.0	\$ 4,770.0	\$ 566.0
Net Contribution %	16%	14%	19%
Net Contribution (\$000)	\$ 13,680.0	\$ 12,454.7	\$ 16,717.5
Opportunity Cost: Contribution Lost to Valid Order Rejection	\$ -	\$ 55.3	\$ 0.9
Net Contribution Adjusted For Opportunity Cost (\$000)	\$ 13,680.0	\$ 12,399.4	\$ 16,716.7

Intended for illustration purposes only. Actual results vary by company. Companies are advised to use their own assumptions and base results on specific organizational practices. ©2000, CyberSource Corporation.

Conclusion

Fraud on the Internet can be effectively managed—just as it has been in retail and mail order/telephone order environments. However, businesses are advised to consider the unique nature of Internet fraud risk and ensure they are prepared to screen orders with systems designed for this purpose.

Systems or policies that are overly stringent and rely only on traditional authorization systems increase exception processing costs and reject valid orders. Liberal strategies based only on traditional authorization systems fail to effectively control fraud and may carry other financial risks.

For these reasons it is recommended businesses use a commercial fraud screening system designed for Internet use. Internet fraud screening services, such as CyberSource Internet Fraud Screen enhanced by Visa, have proven effective in augmenting card authorization systems to minimize merchant risk and maximize sales. By using such commercially proven systems merchants can enjoy safe, secure operations on the Internet.



Implementing Your Internet Fraud Screen System

CyberSource provides the services and support required to implement a real-time Internet fraud screen solution that will reduce operating costs and increase customer satisfaction. In addition to tax services, CyberSource offers a full suite of commerce transaction solutions and global professional services.

The CyberSource eCommerce Transaction SuiteSM

The CyberSource eCommerce Transaction SuiteSM includes: payment and tax calculation services that support international sales in over 170 currencies; Internet Fraud Screen enhanced by Visa to manage Internet or call center transaction risk; stored value services to support Internet-savvy gift certificates, gift cards, and other stored value applications; and fulfillment services to support physical and digital fulfillment of products. CyberSource can also provide the professional services and 24/7 support required to implement and maintain your commerce operations systems.

Maximum Flexibility

CyberSource offers the flexibility to implement and manage services in-house using a local server and transaction software. Customers can also outsource their services by connecting business systems to CyberSource data centers via the CyberSource Component. For maximum operating and financial flexibility, CyberSource offers a combination of both solutions.

Our Customers

CyberSource commerce-enables many of the Internet's top sites, including Amazon.com, BUY.COM, Compaq Computer, nike.com, VarsityBooks.com, Wrenchhead.com and many other leading businesses that sell online.

Total Solution

See how CyberSource can help you implement commerce transaction solutions today. You'll maintain high levels of customer satisfaction and complete control of your back office processing. For details, visit our Web site at www.cybersource.com, or contact our eCommerce operations consultants: USA 1-888-330-2300; UK +44-1932-871500.

Commerce Site Developers

Download the CyberSource Component and complete documentation at www.cybersource.com.