Beating the Dot-Cons: How to Minimize Exposure to Internet Fraud

DEBORAH HRBEK

DEBORAH HRBEK is an attorney with Beck & Arad in New York, and Of Counsel to Hewlett Beck & Arad in the British Virgin Islands.

The advent of electronic commerce has brought with it unique advantages and singular pitfalls. The online shopper can make purchases from the comfort of home, and online vendors, or "e-tailers," can offer products and services to consumers all over the world. Not surprisingly, this enormous new marketing opportunity has brought with it concomitant opportunity for "virtual" crime.

It is relatively easy, and at the same time relatively safe, for bad people to commit fraud over the Internet. Cyber-crimes can be committed anonymously from any place the perpetrator has Internet access; thus it is remarkably simple, even for an unsophisticated electronic con artist, to escape detection.

Identity theft, for example, is particularly dangerous in today's world, where a stolen or computer-generated credit card number can be used to make purchases online. Someone can use your credit card number to make an unauthorized purchase while you have the card in your wallet. If you don't know your credit card number has been stolen, you can't report it to the issuing bank until you receive your statement. A cyber-thief can often use a stolen credit card number on the Internet well beyond the 24-hour period that it takes a cardholder to discover and report the loss of a credit card.

Moreover, even if a card has been reported stolen and the online transaction is denied, the consequences for the cyber-crook are minimal. It is virtually impossible to trace electronic users unless they voluntarily provide accurate personal details to the e-tailer. Credit card e-fraud is considerably less risky than attempting to make a purchase in a bricks-and-mortar store using a stolen credit card, where a declined credit card could draw the police.

FRAUD BY ONLINE VENDORS

Consumers often do not have the same confidence in Internet vendors as in stores at the mall. A website could be here today and gone tomorrow. It is one thing when popular established businesses simply expand onto the Internet, and use a website to supplement their storefront retail outlets in order to broaden their market base and their accessibility. Barnes&Noble.com and LandsEnd.com, for example, are considerably more likely to succeed in their online ventures than a purely web-based competitor.

Traditional businesses with familiar storefronts have the advantages of both trust and goodwill that new Internet-only businesses frequently lack, barring the rare exception: well-known and relatively well-established companies like Amazon.com. Consumers gain added assurance from the knowledge that there is a solid, tangible entity to which they can return an item, or complain to if the item never arrives.

To a certain extent, an online consumer's fear of fraud is somewhat unwarranted. Online shoppers can protect themselves against online scams by simple consumer protections. Credit card association rules protect cardholders when they conduct remote transactions. Credit card transactions carried out over the Internet are considered equivalent to mail order/telephone order (MOTO) transactions. In such cases, the cardholder always gets the benefit of the doubt. The online merchant has to provide substantial proof that the ordered item has been delivered (such as a delivery confirmation receipt from a reputable courier company, signed by the cardholder), or the cardholder is entitled to a credit.

There are a number of simple ways online consumers can minimize the risk of falling victim to Internet fraud.

- Never pay by cash. A request for cash is suspicious, and should be a clear indication of intent to defraud.
- Use a credit card to pay online whenever it is available. Credit card association rules provide recourse for disputed transactions that may not be available for other methods of payment.
- If you do not have a credit card, or the online merchant does not accept credit cards, insist on paying cash-on-delivery (COD). Alternatively, use an escrow service.
- Exercise due diligence before making a purchase online. Since you are unable to see the online vendor's physical place of business, use all other available resources to assess the quality of the e-tailer before you buy. Review the website carefully, and make sure that it looks professional. Do not be misled by impressive graphics, however, as it is neither difficult nor expensive to create an attractive website. Signs of professionalism include statement of standard terms and conditions, a clearly stated privacy policy, clearly posted shipping and return policies, and a descriptive "About Us" section.
- Do not place an order if you are unable to find e-mail and/or telephone contact information on the website. Call or e-mail the e-tailer directly to deal with any questions you have about the product or the terms of the sale. It is certainly a good sign if someone answers the telephone, returns your call, and responds to your e-mail. Ask questions about the product to make sure you are dealing with someone who knows the business. Keep a record of the seller's physical address, telephone number, and other identifying information, in case you need to follow up later.
- Make a note of the name and contact information of the payment processor. In many cases, a company other than the online vendor is responsible for processing the transaction, e.g., an e-commerce payment processing company such as Authorize.Net™ or Planet Payment™. Name and contact information should be clearly posted on or accessible from the e-tailer's buy page (i.e., the payment page on which you enter your credit card information).
- Use sites like Network Solutions® (www.networksolutions.com or www.uwhois.com) services to find out in whose name the site is registered. See if there appears to be any connection between this name and the apparent owners of the business conducted on the website, and ask for clarification if there is not. Print out the page so that you know whom to follow up with if things go awry.
- Be particularly wary when making online purchases from certain types of businesses associated with a higher-than-average incidence of fraud. These include auction sites, buyers' clubs, online magazine subscriptions, business and employment opportunities, advance fee loans, credit card loss protection plans or credit repair services, pyramid and multilevel marketing schemes, scholarship search services, sweepstakes and prize offers, Internet access services, and computer equipment and software suppliers.
- Beware of any offer that appears too good to be true. As the phrase goes, it probably is. Fraudulent offers often involve very low prices, free products that require only payment for shipping, or extremely low-priced travel packages. These may be covers to enable a cyber-criminal to obtain your credit card or bank account information, enabling unauthorized additional amounts to be charged to your account.
- Err on the side of caution when considering offers that are available for an unreasonably limited time. You may find you are dealing with a fly-by-night e-con artist.
- Read the fine print to ensure that you know and understand all the terms and conditions associated with your online purchase. If you have any ques-

tions, clear them up directly with the online vendor before making any payment or providing any personal, credit card, or bank account information.
- Never provide your credit card, bank account number, or other account details to anyone who requests this information for identification purposes only, or to enable a sweepstakes company to pay you your winnings. No legitimate prize company would ever ask for this type of information.
- Never provide your credit card information over the Internet in any form that is not secure. Security typically takes the form of the payment processing company's use of an encrypting technology such as SSL (Secure Socket Layer). If you are in doubt, ask the online vendor to describe its security measures before you make a purchase.

FRAUD BY ONLINE CONSUMERS

Fraud by illegitimate buyers is becoming increasingly common, although this type of Internet fraud tends to attract less attention from both the public and the press. Internet merchants need to remain vigilant, and carefully monitor transaction activity on their websites. Credit card issuing banks treat Internet-based credit card transactions as MOTO (mail order/telephone order) or "card-not-present" transactions. This means that the same rules that apply to credit card purchases made by the telephone or via mail or fax apply to Internet-based credit card transactions. The practical consequence is that online sellers bear the entire risk for credit card fraud where payment is made by credit card online.

Online merchants often make the mistake of thinking that approval of a credit card transaction by the payment gateway means that the transaction is legitimate. *Authorization is no guarantee that a card is not being fraudulently used.* Generally speaking, when an online vendor receives an authorization for a particular transaction from its payment gateway provider, all that is being verified is: 1) that the card has not been reported lost or stolen; 2) that the card number is being used within the credit card's valid dates; and 3) that there is a sufficient credit balance to cover the amount of the transaction.

Authorization is no protection, for example, against:

1. A thief who has obtained a valid credit card number and expiration date but not the card itself (so that the actual cardholder does not know that the card is being used and has not made a report to the issuing bank).
2. A thief who has stolen a credit card and is using it immediately, before the card has been reported lost or stolen.
3. Cardholders who are misusing their own credit cards to make purchases over the Internet with no intention of paying for the goods, such as a cardholder who is familiar with and intends to take wrongful advantage of the MOTO credit card association rules in order to fraudulently dispute a legitimate transaction.

Internet merchants can reduce their exposure to fraudulent credit card payments online by following some fairly simple practices:

- *Know your product; know your customers.* Examine every transaction carefully, and develop a feel for your typical customer. Watch out for unusual transactions. For example, when reviewing daily transaction activity and certainly before shipping, investigate further if you notice multiple orders from the same address or the same foreign city. As your online business evolves, you will develop more of a feel for your website's own typical transactions, and it will become easier to spot unusual activity.
- *Monitor your transaction activity closely.* Review your transactions daily, and investigate any suspicious transactions. Look carefully at all the details provided by your payment gateway provider. Bear in mind items identified as potentially suspicious transactions below.
- *Use Address Verification System (AVS) where available.* Ask your payment gateway provider how to use AVS. Credit card associations provide AVS for cardholders resident in the United States. AVS compares the address provided by the customer on your website's buy page with the billing address associated with the credit card. Sometimes these may be legitimately different (e.g., "Ave." versus "Avenue") but it is always worth investigating if no match is found. See the tips on how to investigate below.
- *Develop your own rules.* Once you become aware of a certain pattern of suspicious transactions, develop rules to reduce your risk. For example, automatically decline orders from risky coun-

tries, or insist on a faxed copy of the credit card used before shipping overseas.

- *Use registered mail or a reputable courier service for shipping.* This will enable you to prove delivery in the case of a fraudulent chargeback request by a dishonest cardholder.
- *Post a fraud-screening warning.* Consider posting a notice on your website informing visitors that the site has anti-fraud safeguards in place, and that you will prosecute fraudulent orders to the full extent of the law. This may help scare off some perpetrators.
- *Never process transactions for anyone else through your merchant account.* Processing transactions for anyone other than your own company is known as factoring. You incur substantial additional risk of fraud if you do this.
- *Consider the type of product or services that you offer online.* Certain types of products or services make merchants more vulnerable to Internet fraud than others. Downloadable products or services, for example, carry a high risk of fraud, since actual delivery is difficult to prove. Goods such as electronics, which have a high resale value, also pose a higher-than-average fraud risk.
- *Make sure that your online buy page is secure.* Encouraging your customers to provide credit card information on anything other than a secure server is irresponsible, and makes it easier for cyber-criminals to obtain valid credit card numbers for fraudulent use. The more common this practice becomes, the more likely it is that your online business will be victimized this way in the future. Do your part to preserve your customers' privacy. This is also a good business practice; it encourages consumers to feel confident in making an online purchase from your site.
- *Implement a holdover policy.* Refrain from processing transactions until 24 hours from the time they are submitted, and obtain a second authorization at that time. This gives you additional time to investigate, and additional time for a stolen card to be reported to the credit card associations.
- *Always apply a rule of thumb: If in doubt, verify; and if you can't verify, void.* It is generally better to sacrifice a legitimate sale than to incur the risk that you are being defrauded. Even if the dollar amount of the transaction makes it seem worth the risk, bear in mind that a high chargeback rate can affect your ability to maintain a merchant account facility (the special bank account that enables you to accept credit cards).
- *The best defense is common sense.* Trust your instincts, and use your common sense. If a transaction doesn't feel right, investigate.

Potentially Suspicious Transactions

As an online vendor, you are the best judge of what constitutes an unusual transaction for your business. There are certain types of transactions that should be a red flag, no matter what your business is.

Watch out for:

- Multiple transactions on the same card or from the same address within a short period of time.
- Multiple orders from the same foreign city within a short period of time.
- Unusually high dollar volume transactions.
- Orders for unusually large quantities of goods.
- Orders for which the customer is willing to pay more for expedited delivery, or other indications that the customer does not care about costs.
- Orders for which the shipping address is different from the billing address.
- Transactions from countries that generate a greater-than-usual incidence of Internet fraud, such as Indonesia, certain Eastern European countries (e.g., Bulgaria, Romania, and the former Yugoslavia) and certain sub-Saharan African countries (e.g., Nigeria).
- Orders for which e-mail addresses differ from the cardholder's name.
- Orders from free e-mail domains.
- Orders requesting shipping to a post office box.

How to Investigate

Do not settle or ship goods in relation to any transactions that look unusual until you have verified that the transactions are valid. There are several simple ways to investigate suspicious transactions.

Call the telephone number provided by the customer on your online order form/buy page to make sure it works. If someone answers, get the name, and politely let the person know you are calling to verify the purchase. A fraudulent user is unlikely to provide a real name and

telephone number. If you cannot contact the buyer by telephone, or the number does not work, do not process the charge.

If you do get through to a person on the telephone but you are still suspicious, try to see whether the buyer has the credit card in hand—ask for confirmation of the issuing bank, for example. Or ask for the three-digit extension on the signature line of MasterCard® or Visa® credit cards, or the four-digit number in the center of an American Express® card. You should soon get a sense of whether or not the person is in possession of the credit card used.

If you are still suspicious, ask the customer to back up the order with a fax copy of the credit card and cardholder signature.

If you are unable to verify a suspicious transaction, simply void the transaction.

STANDARD BANK RISK MANAGEMENT PRACTICES

Banks and other financial institutions have viewed the advent of e-commerce as somewhat of a mixed blessing. The banking industry stands to benefit from the success of e-commerce, as increased electronic transactions translate into more money flowing through commercial bank accounts. That said, the banks have been quick to recognize the unique risks associated with Internet-based credit card transactions.

Under credit card association rules, which tend to protect cardholders, it is the merchant (and ultimately the bank if the merchant becomes insolvent) who bears the risk of reimbursing defrauded cardholders who fall victim to cyber-thieves. This is the case whether the perpetrator is a fraudulent merchant conducting an online scam, or an individual using another person's credit card to make unauthorized payments online. Additionally, banks are obligated by banking regulations to take appropriate measures to prevent use of their account facilities as conduits for illegal activity, e.g. money-laundering, whether perpetrated online or offline.

An acquiring bank is a bank that permits an individual or a company to set up a "merchant account" at the bank, enabling the account holder to accept credit cards. Acquiring banks have generally adopted a cautious approach when considering whether to permit a client to accept credit cards online, in particular for e-tailers who want to conduct business internationally. This is because of the acquirer's potential liability to defrauded cardholders, and their professional obligations under applicable banking regulations.

In practice, this means that banks tend to impose risk management procedures in connection with online merchant accounts in order to minimize the risk of loss resulting from Internet fraud. Generally speaking, the availability of merchant accounts for Internet-based transactions is restricted to online vendors who have relatively low-risk online business models. For example, acquiring banks may maintain lists of prohibited businesses and lists of prohibited countries, for which Internet-based merchant accounts will not be opened barring exceptional circumstances.

The bank may demand a security deposit and/or the maintenance of a chargeback reserve account from the merchant account holder, to cover credits and chargebacks not promptly or voluntarily dealt with by the online merchant. A chargeback reserve account generally constitutes retention for a certain period of time of an agreed-upon percentage of the transaction volume conducted by the online merchant.

Before permitting a merchant to open a merchant account for processing online credit card transactions, banks tend to conduct extensive background checks on the beneficial owners of the company applying for the merchant account. Essentially, companies seeking such banking privileges are treated as if they were applying for a loan. This is because, in essence, e-tailer processing of such transactions through the acquiring bank's facility amounts to a loan, in light of merchants' and ultimately banks' obligations to cardholders.

RECOURSE FOR VICTIMS OF ONLINE FRAUD

Many victims of Internet fraud are justifiably frustrated at lack of interest or lack of response from law enforcement authorities, particularly compared to responses to conventional street crime or white-collar crime. It is not so much that the police or other enforcement arms do not want to help. The problem is that traditional law enforcement techniques are not effective for dealing with the new breed of electronic criminals—the virtual criminal does not leave fingerprints. Moreover, law enforcement agencies are often confined to geographic jurisdictions and authority, which provides a tremendous advantage to cross-border activities of cyber-criminals.

As we wait for development of more advanced law enforcement techniques, and for jurisdictional limitations to be lifted when necessary and appropriate, atten-