



SECURITY

[TechNewsWorld](#) > [Security](#) | [Read Next Article in Security](#)

May 25, 2006 08:13:37 AM

Please note that this material is copyright protected. It is illegal to display or reproduce this article without permission for any commercial purpose, including use as marketing or public relations literature. To obtain reprints of this article for authorized use, please call a sales representative at (818) 461-9700 or visit <http://www.ectnews.com/about/reprints/>.

CASE STUDY

Battling E-Commerce Credit Card Fraud



By Sandeep Walia
www.EcommerceTimes.com
Part of the ECT News Network
05/25/06 5:00 AM PT

[E-Mail Article](#)

[Back to Online Version](#)

Without question, cyber crime is on the rise, and criminals are becoming increasingly sophisticated. As global dependence on e-commerce increases, automated fraud screening will continue to be a crucial first line of defense.

The Internet is still a very dangerous environment for conducting business. Lurking in the cyberspace shadows are criminal masterminds bent on stealing personal information and credit card numbers to further fund their activities. Almost daily, stories involving new worms, phishing scams or large security breaches headline the news. According to [Celent Communications](#), an international consultancy group, the United States alone faces US\$3.2 billion of online credit card fraud by 2007.

A recent survey conducted by [RSA Security](#) (Nasdaq: RSAS) found that nine out of ten Americans want their banks to monitor their online accounts for suspicious behavior. The poll went on to report that 79 percent surveyed said they were less likely to respond to e-mail from their bank because of worry over phishing scams -- up nine percentage points from 2004. Although Internet scam artists for the most part target individual consumers, businesses are frequently on their hit-list as well.

US Digital Media

One company recently targeted by cyber thieves is [US Digital Media](#), an online wholesale distributor of optical media products with operations spanning the globe.

US Digital Media lost upwards of \$200,000 even though strong security measures were in place such as random manual verification of orders and credit card AVS, which matches a credit card number with the billing zip.

On one extraordinary occasion, US Digital Media was targeted largely because of the type of merchandise it offers and the ease of ordering online. The company was alerted to the situation


after several suspicious transactions took place involving large orders to an unorthodox address. Suspicions grew because orders were coupled with instructions for next day delivery. Alane Pignotti, general [manager](#) of US Digital Media, says they always pay special attention to large orders marked next day delivery especially if the order is coming from a new or unrecognized customer.

The authorities were alerted, and it was quickly determined that the person placing orders was using stolen credit card numbers. Because of the large volume of blank recordable CDs (CD-Rs) involved, an initial investigation revealed that at the center of this scam was a seasoned international movie pirating organization. Since movie pirating is a federal crime, the case was immediately handed to the FBI.

The FBI had been tracking this group for sometime, and this was the break they were looking for. In an unconventional request, the FBI asked US Digital Media to get involved and help nab this crew. US Digital Media agreed, and a sting operation was organized. US Digital Media was to wait for the suspect's next order and comply by sending the shipment. To minimize the risk of losing additional merchandise, the actual shipment sent to the movie pirating organization consisted of wooden pallets in place of CD-Rs. The FBI agents set out disguised as DHL workers complete with uniforms, name tags and the trademark bright yellow truck.

The trap was set and the waiting began. After only a few days, an order destined for Chicago was placed and the agents sprung into action. At the moment of delivery, the suspect wasted no time and began opening the shipment as it came off the truck. The agents watched in wonder as the suspect ran across the street to a nearby pay phone. Deducing the situation, the FBI phoned US Digital Media and confirmed their hunch -- the suspect was complaining to [customer service](#) that he received the wrong package. When the situation finally clicked he turned around, only to see himself looking down the barrel of a gun with orders to get on the ground.


Automated Fraud Prevention

The experience with the FBI forced US Digital Media to re-evaluate its online purchasing model. Because all orders were processed manually before being transferred to shipping , opportunity for human error was a substantial threat. After evaluating several options, US Digital Media chose to deploy the [Ignify](#) eCommerce platform. US Digital Media chose this particular platform based on the automation that the system could bring to US Digital media as well as the special heuristic screening methods that automatically flags orders by cross-referencing a list of over 10 transactional behavioral points signaling abnormal purchasing behavior. Over time, the system is designed to learn buying patterns of customers, adding an additional layer of security.

The Ignify system is configured to work with automated fraud screening. All orders that come in go through a combination of parameters that fraud orders meet. Orders that meet a certain risk level are then assigned to a fraud bucket while other orders are automatically released for processing. The orders in the fraud bucket are reviewed and a US Digital Media customer service representative calls the customer to verify the order. The combination of automated

screening via automated system monitoring and a second level of telephone verification has completely eliminated customer fraud at US Digital Media.



Fighting Back

Although the case involving the FBI is not an everyday occurrence, as multi-channel marketing  continues its surge, online fraud prevention becomes more and more crucial to any organization.

There are several simple precautions that can minimize fraud significantly with little or no investment:

- Ensure that you have AVS (Address Verification System) checking that can be done automatically when the order is placed.
- Screen orders that meet certain criteria for an additional level of verification, and follow this process consistently every day.
- Pre-authorize credit cards automatically when the order is placed.
- Ensure that your fraud prevention is not limited to credit card orders. Bogus checks and Western Union transfers also have a high incidence of fraud.

Bottom Line

Without question, cyber crime is on the rise, and criminals are becoming increasingly sophisticated. As global dependence on e-commerce  increases, automated fraud screening will continue to be a crucial first line of defense. By identifying questionable transactions on the fly, organizations can better focus resources towards their end goal -- selling product to you and me at a reasonable price with good customer service. 

Sandeep Walia is president of [Ignify](#), a leading provider of e-commerce solutions targeting the SMB market segment.

[▶ Read Next Article in Security](#)

Copyright © 1998-2006 ECT News Network, Inc. All rights reserved. See [Terms of Use](#) and [Privacy](#) notice. [How To Advertise](#).