

## Online Gaming Company Reduces Credit Card Fraud by a Factor of Ten with ieSnare

### Executive Summary

UltimateBet™, a leading gaming company, ran into big trouble when an online poker company it owns was suddenly beset by extreme fraud. Credit card chargeback rates jumped to higher than 10% of deposits, an unsustainable level equating to roughly 20% of its gross revenues. UltimateBet's fraud managers were overwhelmed - they had no tools with which to identify the perpetrators and stop them. If a solution was not found quickly, UltimateBet faced the possibility of financial failure.

Today, UltimateBet not only overcame this enormous challenge but is growing rapidly and has become one of the leading forces in online poker. The company's fraud problems subsided after it implemented the ieSnare™ system, a unique back-end fraud-control solution from iovation that is powerful, easy to use and fast. ieSnare combines innovative device-fingerprinting technology with a robust database that associates devices and accounts.

ieSnare helped UltimateBet get a handle on fraud. It gave UltimateBet access to a centralized database that collected information about the devices connecting to UltimateBet's network. Powerful research features provided UltimateBet with a way to have vision into whether the devices had been used for fraudulent activities, and to make associations between devices and customer accounts. UltimateBet was able to devise its own set of rules governing end-user interactions, and retain control over the environment.

Within a matter of months, UltimateBet was out of trouble. As a result of using the ieSnare solution, UltimateBet's fraud level fell dramatically, shoring up the company's bottom line. The chargeback rate dropped to under 1.5 percent, and is now below .43 percent – a phenomenally low level, particularly in the multi-player online gaming industry. In addition to fraud via credit card chargebacks, UltimateBet was also able to use ieSnare to tackle fraud due to collusion and other unwanted behavior. ieSnare was so effective in reducing the burden on UltimateBet's fraud managers that headcount could be lowered significantly, further helping the bottom line.

Credit card fraud is not limited to online gaming. Online retailers, financial service companies, online auction houses, payment systems and other Internet businesses also suffer from crushing levels of fraud. ieSnare presents an innovative solution that could be useful for any of these industries. Like a credit bureau for devices that connect to the Internet, ieSnare's centralized database of device information (known as the Device Reputation Authority) can be shared making it a powerful force in the fight against fraud.

### **The Challenge of Online Credit Card Fraud**

Most online businesses are all too familiar with fraud and other delinquent behavior that is currently pervading the Internet. One of the most common forms of fraud is when stolen credit card numbers are used to make online transactions. These stolen numbers are often passed among rings of criminals operating in several countries. Once the owner of a credit card account discovers an unauthorized charge on their statement and reports it to their credit card company, the credit card company initiates a process called a chargeback, whereby the money paid to the online merchant is reversed out of its account and refunded back to the credit card holder. The online merchant loses money with each fraudulent transaction – often after real goods and services have been provided.

The amount of online credit card fraud in the U.S. was estimated at 2.3 billion in 2003 and 2.6 billion in 2004, according to Mindwave Research. And it is expected to get even worse, as ecommerce sales forecasts continue to show growth in excess of 20%.

Credit card fraud is significantly damaging to the ecommerce sector as a whole - the success of the online economy is highly dependent on the public's perception of the security of their interactions. In late 2002, the Gartner Group and Harris Interactive released the results of a survey showing that 7% of online adult customers had already reported being victims of credit card fraud by October of 2002.

Of all businesses, online gaming is perhaps the most prone to credit card fraud. Online gaming operations resemble banks, in that deposits and withdrawals are permitted. However, in multiplayer online gaming, money can be transferred between end users much more freely than it can with online banks. "There are very few industries that I can think of where there are as many ways to defraud a site as there are in online gaming," said Jon Karl, Vice President of Marketing and Business Development at iovation." In gaming, you can move money very easily from one legitimate account to another and the ability to determine what's legitimate and what's not is very difficult."

The industry chargeback norm in the online gaming industry is between 1.25 and 2 percent of deposits. This means that if, say, 100 million dollars is deposited by players over a matter of months, the chargeback rate would be roughly 1.5 to 2 million dollars.

UltimateBet, a major online gaming company based in Antigua, operates an online poker site called Ultimatebet.com. At one point, this site was suddenly beset by credit card fraud so severe that UltimateBet's chargeback rate shot up in excess of 10% of deposits – a level equal to about 20% of its gross revenues. This amounted to millions of dollars of losses in a matter of months. "Not only were we taking the hit from the money coming into the site, but we also couldn't reclaim money lost to other people at the table who were playing legitimately," said Carolyn Heick, fraud manager at Excapsa, Inc., the software development company for UltimateBet. "In essence, we were paying it out twice."

The fraud worked this way: a perpetrator creates say, four accounts on Ultimatebet.com, and makes deposits to the new accounts using the information from four stolen credit cards. A group of conspiring players plays at the same online poker table together using these accounts. All of them just happen to lose most of their money

to one player, another conspirer. To make matters worse, some of the money is lost to legitimate players at the same table. The winner cashes out of the system, gets a check mailed to them and cashes the check. By the time the legitimate owners of the credit cards discover the unauthorized transactions, and the credit card company reverses the charges, the money is long gone.

Heick suspected that the same person or group was perpetrating much of the fraud when she started seeing the numbers of chargebacks jump suddenly by a factor of ten in six months. "We were seeing a lot come back in a very short period of time, so it was obvious that it was a group of people that had a list of stolen cards," she said. "They would deposit money and play using new accounts, and I had no way to track it and prove that these were the same people."

UltimateBet tried several common fraud management methods, including spending massive resources on audits, on heuristic analysis of game play, and using existing solutions for credit screening, but nothing seemed to work. To complicate matters, UltimateBet needed to find a solution that would fix the problem of fraud without violating the privacy of its customers – a critical concern for both the site and its consumers.

As time went on, new fraudulent accounts were being spawned incessantly, and the chargeback losses were becoming unsustainable. "We were at a critical crossroads," said Heick. "We knew if we didn't fix this problem UltimateBet was going to go under."

### **The ieSnare Solution**

UltimateBet needed help.

iovation's team determined that the problem could not be stopped by simply identifying and closing down accounts used for fraud. "UltimateBet had no way to stop perpetrators from simply creating new accounts and continuing their fraud activities," said Karl.

In response to UltimateBet's situation, a unique solution was developed called ieSnare, which identifies and records the devices that are used to connect to online companies, as well as the accounts with which those devices are associated. "The way we saw it, every connection to their site had to come through a device such as a computer," said Karl. "If we could develop a way to give companies a simple view of which devices were being used to access their online network, and which accounts those devices were using, then they could shut out the devices that are associated with fraudulent accounts."

At its most fundamental level, ieSnare tags the computers and other network devices that are being used for fraudulent or other unwanted activities. The ieSnare system is comprised of two primary elements:

- > **DevicePrint™**, a system that uniquely identifies devices using proprietary methods. DevicePrint essentially uses hardware, software and network information to create a unique profile or digital fingerprint for each device that accesses an online network. The digital fingerprint is extremely accurate and resistant to manipulation.
- > **The Device Reputation Authority™** is a centralized database of device identifiers. It includes information about the reputations of devices as well as the relationships between device fingerprints and network specific end-user account identifiers. The device identifiers contain no real customer information, and therefore limit privacy concerns for both the subscribing companies and end-users.

Companies subscribing to ieSnare activate the DevicePrint application either by including a small code set in their own downloadable application, or through ActiveX and other controls. This makes it possible for encrypted DevicePrint identifiers to be created when a device logs in to the company's network. A unique account identifier is then appended to the DevicePrint identifier, and that information is passed on to the Device Reputation Authority.

Each company establishes its own sets of rules regarding specific end-user interactions. For example, one company might create a rule that no more than three accounts can be set up by the same device on the company's network. If a device tries to set up more than three accounts, the company is to be notified.

At key end-user interaction points, such as account creation, login, purchase, and other touch points, the subscribed company automatically reaches out to the Device Reputation Authority to determine, according to the subscriber's own rules, whether or not to proceed. The Device Reputation Authority returns simple 'proceed' or 'stop' responses. If suspicious activity worthy of investigation is encountered, ieSnare can notify the subscribing company. The subscribing company is left to make the ultimate business decision about whether to exclude a device or account, or what other action to take.

Subscribing companies are provided with a simple interface into the database based on HTML and Simple Object Access Protocol (SOAP). The interface allows them to view the relationships between devices and account activity. It also allows them to maintain their own rule sets, update their own device reputation information, run queries and generate reports.

## **The Benefits of Using ieSnare**

### **Creates a negative database of devices without compromising customer privacy**

Historically, the online gaming industry has kept negative databases – that is, databases of people who should not have access to the system because of unwanted behavior in the past. ieSnare uses a slightly different approach – it keeps track of information about *devices* rather than people. This unique approach is based on the fact that a person who is willing to defraud an Internet organization may have many different aliases and may be using stolen credit card information, but they are likely to use the same group of devices. "It's the first solution I've seen that keeps a negative database of devices," said Jim Ryan, president and CEO of Excapsa, Inc. "It gives us the ability to add an extra degree of security around the organization by not only locking out the person, but locking out the tools that they use to defraud the system."

Significantly, the information kept in the Device Reputation Authority is only related to particular devices. No specific personal customer account information is shared or even recorded in the database. This means that different subscribers can freely share device reputation information from the database without compromising customer privacy. The only information shared is the knowledge that a device has been reported "bad" on a network somewhere – and the reason why.

### **Powerful search features provide a simple view of the associations between devices and accounts**

The ieSnare solution includes powerful search features that let fraud managers do research into the device database so that they can determine the associations between devices and accounts. "This is a way to view which devices are associated with which accounts, and in doing so, stop perpetrators in their tracks," said Jon Karl of iovation.

Fraud managers can search the Device Reputation Authority in a wide variety of ways. "I can look at an account and ieSnare will show me all the devices that account has ever logged in with," said Heick. "And I can see every account that has logged into any known device. It really helps us dig down deep to see what the smart fraud guys are doing."

This deep research capability is especially helpful in discovering rings of people working together. "If you know of one fraudulent person's device, you can use that information to grab everybody," said Heick. "Even though on the surface it looks like only one person with one computer, we can associate the other people in the ring because they let these other people log in using their device."

Once ieSnare was put into place at UltimateBet, the fraud managers were quickly able to start making associations. "We had a group of people that we suspected of being fraudulent from researching their (poker) hands, and we had disabled their accounts so that they couldn't use them to play on our site again," Heick said. "We started monitoring their devices to see if they were trying to create more accounts, and sure enough they were, using the same device. Then we started to see that many chargeback accounts had all logged in from the same device. ieSnare allowed us to shut out their devices so they couldn't log into the system anymore."

The results were dramatic. "We started making many more associations, going 'aha! I knew it was these guys!'" said Heick. "That's when it all came together for us. We were able to prove fraud and stop the groups that I felt were responsible for at least 90% of our fraud at that time."

A high point for UltimateBet was that it was able to bust a huge fraud ring operating in several different countries. "With the help of ieSnare, I was able to go to our two payment processors and say 'Hey, these guys we thought were bad all shared the same devices!'" said Heick. "We came up with about 250 accounts that were all the same group and shut them all down. The lowdown for them is that they're not going to want to invest their time with us."

### **Chargeback rate fell to almost negligible level**

Within a matter of months of installing ieSnare, UltimateBet was able to reduce its chargeback rate enormously. It dropped from over 10% to about 1.5% in about six months, and is currently running below .43 percent. "This is almost unheard of in the gaming industry, and it's very rare for any online transactions," said Karl.

The impact on UltimateBet's bottom line has been tremendous. It happened very fast. "Once we stopped these guys, we were really surprised how quickly things turned around," said Heick. "And it's so much easier to manage now, because as soon as we suspect a ring, we can retain some of the money and return it to the credit card before the cardholder even knows the card information was stolen."

### **Improved bottom line through reduced headcount**

In addition to precipitously reducing chargebacks, ieSnare improved UltimateBet's financial outlook in another way. It allowed the organization to significantly reduce the headcount dedicated to identifying fraudulent types of transactions. "That's a huge bottom line savings," said Jim Ryan of Excapsa.

Many online organizations have fraud management departments with as many as twenty people. At UltimateBet, only two people now handle all of UltimateBet's fraud management, even though the transaction volumes are now much higher than they were before ieSnare was installed.

"I would not be able to do my job as well as I do without ieSnare, and I would not be able to handle the large volume of deposits that we have with just myself and another person," said Heick. "What used to be a 8-9 hour a day process now takes about three hours a day, including trying to link accounts together, make sure that bad people are shut down through all the levels, and figuring out where the money should be."

### **A high degree of control for the user**

The ieSnare solution gives users a great deal of control, and to a very granular degree. Many other fraud solutions on the market are too tight, in that they lock out legitimate business along with fraud. ieSnare is very "tunable", in that the user maintains complete control over how it is used. Importantly, ieSnare has given UltimateBet the confidence to relax some of their restrictions on deposit amounts, resulting in an enormous uplift to their deposit rates without appreciable increases in fraud.

"In essence, all ieSnare does is give the user information that allows them to make decisions and control the environment," said Karl of iovation. Users not only create rules, such as setting what the appropriate number of accounts should be per device, or the number of devices per account, but they can also control, to a great degree, what happens to the offending devices. For instance, rather than denying a device access to the online company's network, it could instead be cut off from using certain account features, such as deposit or withdrawal.

Another benefit for UltimateBet is that the ieSnare device queries can be applied anywhere in the cycle of customer interaction: at registration, on sign-on, when the player is depositing money - anytime the player has an interaction with the server. "It gives users the opportunity to touch a particular individual at various points in the cycle," said Jim Ryan of Excapsa. "I like that because when a player registers, they may not yet be in our negative database. But if they become bad after they've registered, we can still identify them."

### **Easy to install and use**

UltimateBet found that implementing ieSnare on their system was a very easy matter. "They took the support group down for five minutes, and then it was up and running," said Heick. "It wasn't an imposition to us at all."

Learning how to use ieSnare was very straightforward. "Even though you do have a lot of options, it's simplified so that after using it for only five or ten minutes you're a pro," said Heick. "It's pretty self explanatory."

Heick also appreciated that the search system has a very fast response. "It digs through the data quickly," she said. "It's going through so much information, but a reply pops up within moments."

## **Beyond Chargebacks: Controlling Collusion and other Undesirable Behavior**

One other way that online gaming sites can be defrauded is through collusion, whereby individuals playing at the same virtual table tell each other what their cards are, perhaps via a conference call or through instant message services. "You're effectively cheating the other players at the table," said Ryan.

ieSnare helped UltimateBet tackle that problem as well. "We identify those players suspected of collusion, and we flag their devices, so we now know that an individual has been caught colluding in the past," said Ryan. "We now have a footprint of the colluder's computer device, so that whenever they come back, even under a different name, the system has identified their computer."

According to Jon Karl at iovation, ieSnare can be used to combat many other kinds of behavioral problems online, such as rude or abusive behavior in an online community. "Their devices could be tagged as being associated with abusive behavior and their chat privileges revoked," said Karl.

## **Looking Forward to a Bigger Network**

As other online companies begin sharing a negative device database the Internet will become a safer place to do business. Like a credit bureau for online businesses, ieSnare would act as a central repository that is continually updated. The reputation of the devices would be shared among all subscribers through the Device Reputation Authority, exponentially expanding the information about fraud perpetrators without compromising customer privacy.

This is an exciting prospect for fraud managers. "I can't wait to take advantage of a larger network because I know these guys are doing fraudulent activities with as many sites as they can," said Heick. "If we could stop them right away when they try it just once, and prevent them from ever doing it again with any of us, it would be even more invaluable."

## **Conclusion**

With ieSnare, online businesses can now associate the identity of physical devices to any of the accounts that cyber-criminals create, or try to create. This solution has enormous potential to limit fraud and other undesirable behavior in any online business, including financial services, transaction processing, online auctions, online retail and e-wallets. If fraud is reduced in online transactions on a large scale, the entire ecommerce sector could benefit from the restoration of public confidence.

## **About iovation**

iovation, based in Portland, Oregon, develops fraud-management software in high risk industries for companies besieged by significant online fraud issues, particularly stolen credit cards, chargebacks and cyber-crime rings. The company pioneered unique online fraud-detection technology that links users and their accounts with physical devices. iovation currently manages the reputation of over 1 million devices.

For sales inquiries:

Rich Orcutt

+1 503 224 6010 x208

[rich.orcutt@iovation.com](mailto:rich.orcutt@iovation.com)

For general business and partnership inquiries:

Jon Martin Karl

+1 503 224 6010 x202

[jon.karl@iovation.com](mailto:jon.karl@iovation.com)