

The Acquiring Mind

Take Charge Business Consulting, LLC is a full scale consulting firm specializing in merchant credit card acquiring risk, operations, and compliance. TCB publishes this newsletter as a service to the industry. We try to find a balance of articles for law enforcement, sales, risk, compliance, and merchants. We hope you enjoy this complimentary copy.

Issue 8

February 2, 2009

help law enforcement change organized crime laws

Our regular readers will know, TCB takes a very active role in helping law enforcement in any way we can. We have received some requests to bring an issue to the spotlight and ask readers to help out in changing some of our federal laws. This will take people writing to their Congressmen.

Believe it or not, the issue is illegal dog fighting. About now everyone is asking how this affects the payments industry, but it does. I spoke with the investigators working a huge Harris County, Texas case and it was fascinating to learn about the number of

other criminal activities revolving around illegal dog fighting. They said that they witnessed everything from drugs, stolen property, illegal firearms, Identity theft, credit card fraud, you name the offense.

The focus of the investigation was the dog fighting itself. The group was so brutal, the investigators had to break it up when they did so the 187 dogs would not freeze to death in the conditions they



were in. The investigators explained they could have gone on for months retrieving intelligence on other crimes, but the brutality just got to be too much. 55 people were indicted.

Dog fighting is tied into many organized crime groups. The investigators wanted me to send out a plea to all to help get our laws changed to make dog fighting an organized crime under federal law.

Continued on Pg 3



Special points of interest:

- **Changing the Laws Concerning Organized Crime**
- **PCI—Back to the drawing board**
- **Loss and Fraud Trends**
- **The Institute for Fraud Prevention**
- **Acquiring Operations and Risk Webinar Training Series Now Available**

PCI—Can someone Please go back to the drawing board?

The PCI aspect of the merchant acquiring appears to be paralleling US Congress. There is too much red tape and bureaucracy complimented by a whole lot of special interest groups. How do we dig the industry out of this mess? The recent hacks on PCI compliant processors takes me back to a hackers conference I attended a few years back. The hacker demonstrated how to hack into merchant accounts via wireless. He actually held up the what was then the CISP regulations and began laughing at all of us. I

hate to be the one to break it to everyone, but PCI has been a joke to the hacking community for some time now.

The Bureaucracy Spin PCI any way you want to... PCI is just a road map... PCI does not mean you are hack proof... The cold hard fact is the US needs to begin implementing another form of authentication at the point of sale. Render the card number useless and no one will want it.

The argument has been that the issuers do not want to

endure the expense of reissuing cards. Is that not what they are having to do in many of these cases? What about the impact on losses?

The merchant side's argument is that the merchants will not want to spend the money upgrading terminals. What exactly are they paying to the processors for PCI compliance of their own and of the processor? ...financial gain and a false sense of security—much like some of the identity theft monitoring "tools."

Continued on Page 2.



Fraud and Loss Trends

Out of business losses and bust out frauds are the current leaders in loss and fraud types. MAC members are also reporting new twists on the old TYY scheme.

Processors are reporting a rise in the losses due to out of business in 2009. This is not surprising due to the slow down in the economy. Hopefully our readers began shoring up their policies around re-underwriting accounts back in October. For those of you who have been told by your marketing departments for years that credit does not matter in the processing world, well it does now!

Tracking the amount of future sales/services a merchant is taking on is key to the success of your portfolio. Not only should you be underwriting accounts at the application phase, but your team should be actively "re-underwriting" accounts based on volume of future sales/services. You will continue to see huge losses if you have not established a formal policy around future services.

Issuer bust out fraud is still dominating the industry. Due to the rise in business identity theft, these frauds are more and more difficult to identify at approval. Processors are never as worried about bust outs due to the low losses. With banks taking blows in so many other business fronts, you can bet that this will eventually catch up with the acquiring industry. Association rules have already been updated to ensure the issuers have the chargeback rights on their side.

The common threads on the recent bust outs are that the merchant account data typically is not matching the receiving bank information. It is much more difficult now to set up a fraudulent bank account than it is to set up a fraudulent merchant account. Fraudsters take advantage of the fact that they can print their own checks. Since acquirers do not typically call the receiving bank to verify the account information

matches, it is not necessary for them to set up a bank account for each fraud.

The fraudsters tend to use the same cards between fraudulent accounts. A system should be in place within your risk monitoring to tag confirmed bust out cards and search your portfolios for future merchants running these cards. At the bare minimum, when a bust out is confirmed, your investigators should take the additional time to search each card within your portfolio for links to other fraudulent accounts.

The hearing impaired schemes seem to be popping back up with some new twists. Before the schemes involved shipping merchandise which could be easily resold for profit typically to Africa. One would typically see electronic equipment, clothing apparel, high performance auto parts (also used in bomb making), etc. Now we are seeing even special order products and live animals. In most cases a bogus shipping company is being used. Not only is the merchant out the merchandise, but he/she pays the bogus shipper to steal his product.

Another twist seems to be targeting the auto repair industry. We have all seen fraudsters make charges and then ask for returns via cash or check. These involve the fraudster asks for the vehicle to be towed to the merchant's location. The merchant runs the charge and then the fraudster calls back saying the tow is too much and wants a refund via Western Union.

The industry should form a special task force with Western Union and the USSS to build better bridges in getting money recovered. Western Union tends to work well with the Service on these types of cases.



PCI Continued from Page 1

There is a need for security standards and education, but when exactly did things get this out of control? If companies the size of Heartland and RBS WorldPay cannot secure their systems, what hope is there for the auto mechanic, hair stylist, and bookkeeper with no IT staff? PCI is beginning to crush the American dream of owning a small business. Think about it the next time a small merchant goes into bankruptcy due to fines after a hack. We have lost site of the real issues and have accepted a "fix the symptoms not the cause" philosophy.

The issue here is that no one can admit the problem and it is only going to get worse. As Canada moves to chip and pin, the US will be seeing even more. The really bad attacks are not coming within our own borders. We have very little control over what is happening or the outcome of an investigation. Investigators and members of law enforcement are basically useless against a hack coming from Russia. When do we stop calling it fraud and begin calling it what it is...cyber-terrorism?

The merchant industry has pumped millions of dollars into PCI at this point, but the entire system needs to be rethought.

Special Interest

Everyone has an angle on PCI. A great example is the new certification exam called the Certified Payment Card Industry Security Auditor (CPISA) certification put out by the Society of Payment Security Professionals. If you look closer at the SPSP group, dues are paid to the Aegenis Group, a security consulting firm. The exam may be a great tool. However, it is not recognized by the PCI Council. If PCI Council is the entity recognized by the Associations, then they need to be backing certifications. The SPSP's site states they are not affiliated with the PCI Council. You cannot view the SPSP's member companies so it is not clear whether Visa, MasterCard, Discover and American Express involved with them. Are the Associations endorsing this certification?

We would like to see statistics on the PCI companies. The industry is held hostage to high prices through only approved PCI vendors. It is difficult to choose the right one. The RBS and Heartland hacks were both processors certified by Trustwave per documentation on visa.com. It would be a real help for processors to be able to see track records of the vendors. Even if the PCI vendor did the certification correctly, what type of education process is being offered during the process to IT staff which have to support it after the fact?

It is nice to see the entrepreneurs of the world go after the PCI pot of gold, but it would be nice to see some kind of actual solution.



Illegal Dog Fighting/ Changing the Laws—Con't. from Pg 1

The offenders in this case would have been more severely punished had they been able prosecute them with the organized crime statutes. Unfortunately, it is my understanding that all of the dogs had to be euthanized and the offenders face a mere 2 years in jail.

Dog fighting is a huge underground network of criminals. It is organized crime. The investigators explained that any time they were traveling, they would just call their contacts here in Harris County. The contacts would arrange for the investigator to attend a fight wherever he was going to be traveling. It is a widespread issue which obviously attracts the criminals we are all looking for.

I cannot mention the undercover agents names working this case, but they should be commended for all of their hard work and the ability to work such a terrible case. Our hats are off to you and the Harris County District Attorney's Office!

Please contact your Congressmen and ask for the federal laws to be changed. Even if the animal cruelty element of this story does not touch you, this would have been an easy way to get some really bad people off of the streets for a long time had the laws been on our side.

This link provides a list of contact information for the Senate and House: <http://usgovinfo.about.com/gi/dynamic/offsite.htm?site=http://www.lib.umich.edu/govdocs/congress/conemail.txt>

Feel free to contact TCB if you need a form letter.

The Institute for Fraud Prevention

The ACFE featured the Institute for Fraud Prevention in an article in this month's Fraud Magazine and we felt the information was worth sharing with the industry. The IFP works with various law enforcement agencies to develop training and educational materials on financial and white collar crime.

The purpose of the IFP is to globally reduce fraud and corruption. IFP is a non-profit organization with two primary missions: to finance and conduct fraud related research and to educate the public on fraud prevention.

The IFP is currently working with the ACFE to develop a peered review journal so that our community can share fraud prevention white papers. The goal is to groom and develop professors and teachers to fill the void in the education system concerning fraud prevention.

The IFP is holding their conference in conjunction with the International Fraud and Forensic Accounting Education Conference (July 9-11) and the ACFE (July 12-17). The IFP will be meeting on July 11 and 12. The events are in Las Vegas at Caesar's Palace.

If you want to find out more about the IFP or become involved with their research efforts, you can visit their website at www.theifp.org.

Training Webinars for acquirers now available!

TCB has designed a series of webinars addressing issues with acquiring risk and operations. The series is to help continue acquiring education when travel budgets are tight.

Topics of interest will include:

- Risk 101
- Fraud Detection
- Fraud Damage Control and Case Preparation
- Suspicious Activity Reporting
- Customer Service for Investigators in Loss Prevention
- Customer Service for Management in Loss Prevention
- Underwriting 101
- Loss Prevention for Customer Service Personnel
- Acquiring Fraud for Law Enforcement

The webinars are between 45 to 90 minutes depending on the subject matter. The call is accompanied by an online PowerPoint presentation and a short Q&A session at the end of the call. Some of the trainings will also include handouts.

To view schedules and times or to register, please visit our website at www.tcbconsultingonline.com. All webinars are free to members of law enforcement.

If you would like to see subject matter added to this webinar series, feel free to email suggestions to us at service@tcbconsultingonline.com.

Take Charge Business Consulting works to help companies reduce losses while maintaining or increasing application counts. We accomplish this through analyzing processes and systems and providing a road map to best practices in staffing, training, underwriting, monitoring, and target markets. Our staff remains leaders in the industry by making education and networking a priority. Understanding the trends and keeping up with the industry changes is the key factor in our business.

Advertising Space Now Available in the Acquiring Mind!

Law enforcement and industry non profit organizations advertise conferences and seminars at no charge provided space is available.

Contact Deana Sellens at (713) 822-4368 or dsellens@tcbconsultingonline.com for details.



Take Charge Business Consulting, LLC
 P.O. Box 1348
 Houston, TX 77383-1348

Phone: (713) 822-4368
 E-mail: dsellens@tcbconsultingonline.com

Delivering significant and measurable results!

Identify Errors Causing You Losses in Your Residual Revenue

Residual Auditing Services Are Now Available from TCB.

No risk! We get paid only if we find money for you!

TCB has audited many portfolios and to date, we have found losses in revenue on every portfolio we have audited.

The lowest amount identified was \$13.68 (average) per merchant per year. The highest was \$83.40 (average) per merchant per year. How much could we save you?

Savings Calculator

\$13.68	\$83.40
X _____ <i>Insert # Merchants</i>	X _____ <i>Insert # Merchants</i>
\$ _____ add'l revenue/year	\$ _____ add'l revenue/year

You say you check your reporting as merchants are boarded. Do you recheck them on a regular basis? Most errors occur after maintenance by the processor—not at boarding.

Call 713-822-4368 for more information about our NO RISK program!