

The Acquiring Mind

Take Charge Business Consulting, LLC is a full scale consulting firm specializing in merchant 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 4

July 3, 2008



More changes in New York State Taxes— More problems for Online Retailers

New York state strikes again and online retailers are showing some interesting responses. Effective June 1, New York state changed the laws concerning tax collection. This change is affecting affiliates more than anything.

Affiliates are people who operate websites where they link to an online retailer and then the website owner gets paid a commission. The new laws require merchants paying affiliates to collect NY

state taxes from residents of New York. These merchants are not set up for taxing affiliates only buyers. The big guys are working on solutions, but smaller merchants are having a hard time.

Many merchants have chosen to just remove New York state residents while giant Amazon.com has chosen (for the time being) leave the affiliates on and pursue it in the court systems.

NYAffiliates.com is reporting a list of merchant who have

removed affiliate programs from NY state residents. *You can see the list as of July 2nd on Page 3.*

If Amazon's attempts in court fail, many states will follow suit and implement similar laws. There are already 18 states either on the bandwagon or making movements toward the same goals.

Continued on Page 3.



TCB Announces a New Offsite Audit—shore up underwriting/risk inexpensively

TCB is pleased to announce a new offsite auditing service we are providing at an affordable rate. You asked for it and we listened!

With the economy in a down swing, everyone should be concerned by the potential for losses due failing businesses. This service can save you thousands and now is the time to shore up systems and policy.

The audit includes a comprehensive look at underwriting procedures, risk monitoring/investigations procedures and systems, portfolio mix, current losses, and customer service



choice.

Once the data is collected, the audit takes between 3 to 5 days. We review the data for compliance and risk issues. TCB will provide a report of these potential issues and we will provide a list of accounts with potential data entry errors causing losses in revenue. TCB will also review customer service issues surrounding risk procedures and offer suggestions to help

procedures for risk management. We will perform a data entry error scrub on 1500 merchant accounts of your

with merchant retention.

If your information is not formally documented, we obtain the information from your staff through a series of phone interviews. TCB takes pride in offering solutions which fit each client's needs. Your reports and recommendations will be tailored to your business needs.

For an additional fee, TCB can perform an error scrub on your entire portfolio and/or document all policies and procedures according to Association standards. If you provide information on new

Continued on Page 3.

Special points of interest:

- New York State Taxes Causing More Problems for Online Retailers
- New Offsite Audit Designed to Shore Up Risk/Underwriting Inexpensively
- Defcon 16—Hackers Convention in August
- Business Identity Theft—The Basics All Merchants Should Know
- The Acquiring Risk Questionnaire
- Occupational Fraud Report by the ACFE
- Customer Service in Risk
- Helping Law Enforcement with Suspicious Activity Reports
- IAFCI International Conference—Hollywood

DEFCON Hacker's Conference August 8-10



Defcon 16 will be taking place August 8 through 10. Defcon is the biggest hacker's conference in the US. One attends the International Association for Financial Crimes Investigators to network for contacts, but one goes to Defcon to learn.

The final list of speakers has been released and can be viewed at <http://www.defcon.org>. Some of the agenda highlights are Secure Smartcards/Microcontrollers, Attacks on Physical Security, Medical Identity Theft, Cell Phones, Social Engineering, Wiping Evidence the Right Way, and much more!

Speakers include security personnel, attorneys, and of course, hackers. This attendee is always excited to see Major Malfunction on the speaker list. His past demos have ranged from hacking automobile alarms to hotel computers through the television to busting into hotel safes in under 10 seconds.

Who should attend Defcon?

Any IT staff, security personnel, and members of law enforcement should attend Defcon. Law enforcement just beware! One of the favorite games of the conference is Spot the Fed. If you are a federal agent and get spotted, the lucky winner gets to sport a Spot the Fed T-Shirt for the rest of the conference.

The conference fee is \$120.00 USD Cash at the door. You will walk into another universe with projector screens showing live hacking and password sniffing. If you are foolish enough to log into the wireless network, your password will be displayed on the Wall of Sheep.

As you wonder through the venue, you will see lock picking demonstrations and many of the games that go on at Defcon. The conference badges are electronic, so of course there's Hack the Badge.

The Mystery Box Challenge is probably the most intriguing to me. This contest involves breaking into a box. Everything from puzzles, to mathematics, to electronics, you name it is used to hack the box. This game will make you understand the brain power you are up

against if it is used for evil instead of good.

Don't be surprised when you have trouble with your room keys, ATMs and the wireless kiosk. Nothing is safe when these guys are around! Just carry cash and TURN THE BLACKBERRIES AND CELL PHONES OFF!

Why does TCB publicize Defcon?

TCB reminds investigators that there are all kinds of sources and avenues of learning. We are always disappointed to see that almost no one from industry attends. Send 2 people—your risk manager and Network Administrator. Each can translate for each other. If you are not totally computer savvy, don't worry about it. As you begin attending and sitting through meetings you are learning. Every year you get more and more comfortable. Before you know it, you can watch a hack and know exactly what they are after.

If you do decide to go and you recognize a TCB staff member, just give us a wink and keep moving! We hope to see you there!

Business Identity Theft—A Note to Merchants

The subject of identity theft has been beaten into the ground, so this article may not grab the attention of readers until after they search the net as victims. The focus is usually on the individual, but what if you were a business owner and someone stole your business's identity. It can and does happen.

Fraudsters find retail businesses with owners with good to excellent credit, but no website. The fraudster will start a website for the business. The fraudster then applies to accept credit cards under the business name with just a few key pieces of data (Owner's Name, Social Security Number, Date of Birth, Address, and Tax ID). Once the account is approved to accept credit cards, the fraudster begins running stolen credit cards through the merchant account.

If the fraudster has been doing this long enough they will know the thresholds the credit card processors set and can often run a scam for 45 to 60 days. As the credit cards have been run, the credit card processor deposits money into a checking account which the fraudster will empty daily.

Once the credit card holders begin receiving statements showing the

fraudulent charges, they will begin disputing the charges via the chargeback system. The merchant processor will see the chargebacks coming in and attempt to collect the money from the bank account that the fraudster emptied.

Now how does this affect the business whose identity was stolen? When the processor realizes fraud has been committed, they will begin searching for the owner of the business. Once found, collectors begin attempting collection. Processors list the merchant on "MATCH" which tells other processors fraud has been committed by a merchant. This alone can cause a merchant the loss of the ability to take credit cards. Some processors list negative marks on personal credit and D&B. Having a business identity theft can literally put a business under in a very short period of time if not reacted to properly.

Credit card fraud committed against an individual will run a few thousand dollars, but fraud against a business owner can easily reach in excess of \$25,000 and higher very quickly.

What steps should you take as a business owner to protect yourself? Add a consumer statement to your credit

bureau reports that states, "Do not extend credit without contacting me personally at XXX-XXX-XXXX."

Google your name and your business name frequently.

Hire a spidering service to ensure brand/name integrity on the internet.

Periodically pull your credit at least every 6 months and look for suspicious inquiries.

Write letters to your congressmen about the government agencies posting your data online for the world to see. Did you know many states post your business information, your ownership information, and tax id online? Most are free.

Starting your own business takes a person's all. You put your blood, sweat and tears into it and no one should be able to take it away so easily. This is only one way a fraudster can steal your business's identity. There are many more. Be aware of the risks and watch out for you and your employees' futures!

If you have any questions about how to handle the situation as a victim or would like more information on uses for stealing a business identity, feel free to contact me at dsellens@tcbconsultingonline.com.

Merchants who have removed NY affiliates as of July 2, 2008—Continued from Page 1

The problem is that none of the states are attempting to get something standardized set up and smaller retailers cannot possibly keep up with all of the different tax rates.

Anyone reading this, here is the next million dollar idea...a plug and play sales tax calculator fitting into affiliate commissions. I have a ton of these brilliant ideas. Just call me sometime! If you are already using this technology, please contact us so we can refer questions to you.

The following are a list of merchants who have removed New York affiliates as of July 2. Check <http://www.NYAffiliates.com> for updates to the list.

Acorn Media (Linkshare)
 Amerimark (Linkshare)
 Baby Universe (Linkshare)
 Backcountry.com (CJ, Avantlink)
 Binoculars.com (CJ)
 Bodybuilding.com (CJ)
 Brecks (Performics)
 CafePress (CJ)
 CCVideo (Linkshare)
 Celebrate Express (Shareasale)
 Checks In The Mail (CJ)
 Checks Unlimited (Shareasale)
 Collectors' Choice Music (Affiliate Future)
 Compact Appliance (CJ)
 CSN Stores (Shareasale)
 Deep Discount (Affiliate Future)
 DVD Planet (CJ)
 Eastwood Company (CJ)
 eToys (Linkshare)
 Fingerhut (Linkshare)
 FirstStreet



Footsmart (CJ, Performics)
 Gaiam.com (Linkshare)
 Garden's Alive (Performics)
 Geeks.com (CJ)
 Gurneys (Performics)
 Henry Fields (Performics)
 Jewelry Television (CJ)
 J&P Cycles (CJ)
 Justflowers (CJ)
 Karmaloop (Linkshare)
 KB Toys (Linkshare)
 LampsPlus (Linkshare)
 Leaps And Bounds (Performics)
 LinenSource (Linkshare)
 Luggage.com (Shareasale)
 Michigan Bulb (Performics)
 Musicians Friend (CJ)
 MyTwin (Linkshare)
 NetShops
 Northern Tool (CJ)
 One Step Ahead (Performics)
 OnlineShoes.com (Linkshare)
 Oriental Trading (Linkshare)
 Overstock (Linkshare)
 Palo Alto Software (Independent)
 Red Envelope (Performics)
 ReStock It (CJ, Shareasale)
 Ritz Camera (CJ)
 ShopNBC (Linkshare)
 ShoppersChoice (CJ)
 Silhouettes (CJ)
 Spilsbury (Affiliate Future)
 Spring Hill (Performics)
 Thompson Cigars (Linkshare)
 Tিরerack (CJ)
 uBid.com (CJ)

Risk questionnaire

The following Risk Questionnaire was designed to provoke thoughts and bring out questions about anti-fraud controls within various aspects of your organization.

1. Are losses reported to the Board of Directors on a Monthly Basis?
2. Are losses tracked by loss type (Bankruptcy, Fraud, Credit)?
3. Who on the senior management staff owns risk? What audits are performed by this person and at what frequency? How often are systems, policies, and controls reviewed for upgrading—only after a major loss?
4. Is someone cross-trained on every job in your risk and accounting departments?
5. Are overrides or exceptions made by a single member of management or does a committee review high dollar exceptions?
6. Are established steps in place when a fraud involving sales transactions occurs? Is it in line with requirements by federal law?
7. Are established steps in place when credit reversals must take place?
8. What controls are in place for terminal downloads? Can anyone with a loose knowledge or short term employment download a terminal?
9. Does your risk system take ANI numbers into account?
10. Does your risk system take care of all of the basic monitoring criteria: authorization logs, duplicate amounts, duplicate cards, high tickets, high batches, chargebacks, retrievals, returns, entry mode, and foreign card usage? Who in your organization knows the thresholds of this system? How often are they changed?
11. Does your system have indicators for cards used on confirmed fraud accounts?
12. Are parameters the same for new merchants as established merchants?
13. Are merchants performing future services or deliveries monitored the same as "cash and carry?"
14. Are you using the industry list of high risk merchant types or have you developed your own? Are the policies surrounding these types of merchants the same as the rest of your merchant base?
15. Do you have a way for employees to report internal theft? Is it posted somewhere as a reminder? Is there a reward?
16. Are background checks being run on all employees?
17. You're PCI compliant, but are your employees actually following physical security practices properly?
18. What fraud training do you have in place for employees of your company—not just risk?
19. Do you have a Code of Conduct and an Internal Anti-Fraud Policy?
20. Do you have an Employee Assistance Program in place?

Offsite Risk/Underwriting Audit, Continued from Page 1

target markets you are interested in pursuing, we can also report necessary changes to risk and underwriting which should occur to handle the new business and define the risks involved with pursuing these markets.

This offsite audit is designed to be fast and affordable with reasonable solutions designed for your business and we always keep customer service and retention in mind.

To learn more about this audit, please email dsellens@tcbconsultingonline.com or call 713-822-4368.

Occupational Fraud

The Association of Certified Fraud Examiners recently released their report on Occupational Fraud and Abuse. The ACFE defines occupational fraud as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets."

The report covers 3 basic types of occupational fraud: corruption, asset misappropriation, and fraudulent statements. Corruption includes conflicts of interest, bribery, illegal gratuities, and economic extortion. Asset misappropriation includes larceny, skimming, and misuse of company property. Fraudulent statements is misstating financials or employment credentials.

Asset misappropriation occurs the most frequently, but causes the smallest amount of loss. Losses caused by fraudulent statements cause the most dollar losses with the median loss for 2008 at \$2,000,000. On the average it takes 30 months for these schemes to be detected. The median losses for each

category are staggering.

Though banking and financial services tend to have the most cases, the telecommunications industry's median losses are greater than 3 times more than banking. Inside fraud for banking and financial services median loss is \$250,000.

What controls do you have in place to prevent occupational fraud?

Basic anti-fraud controls have a proven track history in reducing occupational losses anywhere from 28-66%. The most effective anti-fraud controls are:

- Surprise Audits
- Job Rotation and Mandatory Vacations
- Fraud Hotline to Report Abuse
- Employee Support Programs
- Fraud Training for Management Team
- Internal Audits
- External Audits of Financials
- Fraud Training for Employees
- Anti-Fraud Policy and Code of Conduct in Place

- Management Review of Internal Controls
- Independent Audit Committee
- Management Certification of Financial Statements
- Rewards for Employee Tips

Lack of internal controls in a company is the number one breakdown in the system.

Occupational Fraud most frequently occurs in the age group of 41 to 50 years of age. The average losses tend to be greater in the 51 to 60 years of age category. Highest losses occurred from employees who have been with the company between 6 to 10 years.

The most disturbing piece of information in the study was there was a direct correlation to salary and fraud rate. Employees making higher salaries commit more in fraud losses than those at lower salary ranges.

The ACFE is a great resource for information on all types of fraud. For more information on joining the ACFE, please visit their website: <http://www.acfe.com>.

Can Customer Service be achieved in risk?

One of the biggest hurdles for every risk manager is to determine where to draw the lines concerning customer service and risk. The retention push is always on, and risk is often a huge factor as to why a merchant leaves a processor.

Investigators are on the phone day in and day out, sounding like a broken record in an attempt to get copies of sales drafts. It's easy to get sucked into the statement, "If you don't send it, we'll just hold your money!" This mentality cannot be tolerated with the competitive nature of your business. Marketing teams work too hard for risk to throw out business.

Risk people need regular customer service training. There is always a tactful way to ask for what you need. Have your people develop the "Yes, but" philosophy rather than always saying no-especially to your sales force. Ask yourself, what would it

take for me to say yes to this? Whatever that thing is should follow, "Yes, but..."

I know it's a little corny for big, bad risk, but put mirrors on everyone's



computer monitors. There should be a smile on everyone's face. Sometimes a quick glance in the mirror during a heated discussion can calm things down.

Ask your staff to put themselves in the merchant's shoes. I am always amazed by how many investigators will be so offended by the fact that a merchant got upset that money was held. My response is always, "Ms. Investigator, I need to hold your paycheck for a week while I verify your Social Security Number." Sometimes pointing out the obvious is necessary to maintain good customer service.

Remind your staff that 999/1,000 merchants are good businesses. You do have to factor in stability with how they are doing business, but the person is not dishonest. No one likes to be treated like a criminal.

Give your staffs a little time off of the phones. Everyone needs an hour or 2 to do research. Being on the phone 8 hours a day will cause your staff to be grumpy.

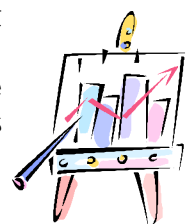
Let your staff sit in with your Sales Team on some cold calls. Selling is difficult and Risk should understand why the sales

offices are so passionate about customer service.

Send your staff out on some installations. One of the biggest eye openers for me as a risk person was I was allowed to go out on an install. I told the merchant everything they needed to know about chargebacks and then some. I was so proud that we would have one merchant totally trained on chargebacks and he was never going to have an issue. Do you know that not even 3 months later the merchant I had personally trained got a chargeback and didn't do anything I told him. He proceeded to tell me that the lady who installed his terminal didn't tell him anything about chargebacks! Needless to say, that experience totally changed my attitude toward Sales.

So Risk, you lost some merchants... Now how do we make it up to Sales and Marketing???

Continued on Page 5.



SAR Preparation—teaching your risk crew to speak English...

All processors should be filing Suspicious Activity Reports on a regular basis. The work has to be done because it is the law, but the number of reports filed poorly is just adding problems for law enforcement.

Are your investigators filing reports that make sense to law enforcement? We find the answer is no, more often than not. TCB liaisons work with about ever law enforcement agency and the complaints we get from all law enforcement officials is that everyone in our industry speaks a different language. The SARs can get put in the bottom of the stack if they have to take time to attempt a translation.

Stop and listen to your team some time. If you invited your mother into your shop, would she be able to understand what was going on? It's bad enough that system notes are so cryptic that other employees can barely follow them. Can you imagine what law enforcement thinks when they are reading your SARs?

The next time you file a SAR, take it to someone in your mail room or receptionist desk. Pick someone who knows nothing about your job and ask them to read it. Then ask them to explain what the crime was. We would be willing to bet that over 75% of the SARs would make no sense to the average person.

Keep in mind that the people reviewing SARs are not trained to do your job. They don't see your system or understand your slang and abbreviations. The concept of keeping someone's money can be called: diverting, holding, freezing... Divert funds where? Did the merchant do it? Is that some kind of laundering?

Take an extra 10 minutes and write your SAR narratives in detail. Leave out industry slang and abbreviations. Make sure you answer Who, What, When, Where, and Why. Help law enforcement help our industry!



IAFCI International conference—Hollywood August 25-29

The IAFCI International Conference is in Hollywood, California this year from August 25th to the 29th. This conference is invaluable to all risk people. Almost every banking institution, financial services providers, and law enforcement agency will be present. Encourage your risk staffs to go and network!

This year's conference's agenda includes classes led by US Secret Service, US Marshalls, Royal Canadian Mounted Police, Philip Morris, US Postal Inspection Service, Department of Homeland Security, Visa, FinCen, and many others. Some of the topics included are Bankruptcy, Data Breaches, Credit Card Skimming, Mortgage Fraud, Global Financial Crimes, POS Fraud, and ACH Fraud.

The International Association for Financial Crimes Investigators is a non-profit international organization, which will provide services and an environment within which information about financial fraud, fraud investigation and fraud prevention methods can be collected, exchanged and taught for the common good of the financial payment industry and our global society.

One of the biggest benefits to the IAFCI is the membership roster you receive as a member. You are instantly connected with all kinds of resources you can reach out to for help.

To join the IAFCI, register for the Hollywood Conference, sponsor, exhibit, or just learn more about the organization, you can check out their website:

<http://www.iafci.org>

Customer Service in Risk, Continued from Page 4.

Ok, reality check... Risk is risk and yes, sometimes we have to put people out of business at Christmas time. You will lose a merchant now and then. How do you do your part to reverse your negative effect?

Well, make more calls of course! It is amazing as to how many risk departments will not call good merchants on a regular basis to warn of potential scams. Typically, risk looks at the account and says, "they can cover a loss" and skips right over it. Make the quick call and inform the merchant of some of the scams going on. Imagine it...you will have a merchant for life and lots of referral business if you save someone a couple of thousand dollars.

Risk Managers—Call your top 10 sales offices at least once a month. Find out what their issues are and LISTEN! So you lose a merchant or two, your sale force will send more accounts into a processor who addresses their issues. These guys are in business for themselves and they do understand. You have to talk to them though!

Last but not least, walk the walk. Make sure your staff knows that you care about your customers. If you do find yourself in a confrontation, shut your door. Don't brag about fighting with customers or sales offices. Losing customers and upsetting sales offices is nothing to brag about.

Achieving a good balance between customer service and risk can be a challenge due to circumstances, workload, and personalities. Once you start walking the walk, you will find your job will be so much easier, employee retention will be better, stress levels will be down, and losses will stay down.



Calling for white papers!

Do you have a case you want everyone to know about?

Do you think you found a new kind of fraud or a twist on an old scheme and want to let everyone know about it?

Have discovered a new industry monitoring or investigations tool and would like to share the info?

Write a white paper! TCB will review and publish qualifying white papers on our website.

The IAFCI Gulf Coast Chapter is also looking for cutting edge speakers for our September conference.

Email white papers to dsellens@tcbconsultingonline.com for review.



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!*

Free investigators
research site!
tcbconsultingonline.com



GULF COAST IAFCI
CONFERENCE
SEPTEMBER 18-19, 2008
NOW TAKING REGISTRATIONS
Early Bird Registration Ends 7/20/08!

The Gulf Coast Chapter of the IAFCI will be holding a conference at the Moody Gardens in Galveston, TX on September 18-19.

This seminar will include:

- Comprehensive 2 Day Seminar
- Complementary hospitality suite Wednesday & Thursday evenings
- Continental Breakfast and Lunch on Thursday and Friday
- A networking social on Thursday evening
- 12 Hours TECLOSE credit for Texas law enforcement officers

Early Bird Registration through July 20th (Fees go up after 7/20)

Law Enforcement: \$130.00, Private Sector: \$145.00, and Private Sector Non-Members: \$160.00

Conference topics include: Credit Card and Check Fraud, Mortgage Fraud, Healthcare Fraud, Data Security, and much more!

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.