

The Acquiring Mind

...wants to Know!

Volume 1, Issue 1
October 10, 2006

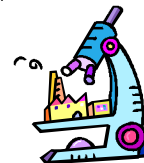


Visa on the Move with ARP reviews

With the implementation of the Acquirer Risk Program in 2004 Visa has been actively making the rounds on member banks to ensure compliance. To date they have conducted 16 reviews. Out of those 7 validated as compliant, 9 are in remediation and there are 6 still in process. Visa's goal is to have all active acquirers with ISO to be reviewed by December, 2007. The purpose of this review is to ensure proper policies and procedures are in place to protect the brand, and to make sure the member is putting forth efforts to ensure the safety and soundness of the payment system. For those of you that are unfamiliar with how the process works. Visa will notify you with written correspondence indicating

that your bank has been selected to participate. In addition they will provide you a list of approved vendors that will be conducting the audit. Please be aware that these vendors although are contracted by you and are paid for by you are there on behalf of VISA. All findings will be reported. Upon completion of the review, areas that are determined to be out of compliance with Visa regulations will require an acceptable remediation plan. Visa will document critical and moderate findings and the time frame for receiving a remediation plan. Also if Visa is to identify serious deficiencies other corrective actions, including fines or Member risk reduction conditions may be implemented to mitigate any

immediate risk of harm to the Visa payment system. Visa has indicated that the common findings are Policies and Procedures that are not formalized, insufficient oversight of the merchant underwriting. Member banks tend to have limited or no access to MIS systems or the merchant files. Visa feels that these reviews will assist both the member and the Agent understand their responsibilities to the payment system. So whether you are a ISO or a member bank refer to the Acquirer Risk Program Standards Guide because your letter could be on its way...



Inside this issue:

USPIS-Another Avenue for Prosecution	2
Expanding Relationships with your Merchants	2
6th Annual MAC Meeting	2
Announcing TCB Consulting	3
A Convention for Hackers?	3
New Resource for Investigators	4

Payment card Industry Data Security Standards... some are running a little late

For the past five years the focus on data integrity has been the topic of every seminar, convention and association meeting. The "seal of PCI compliance" has become better known than the Better Business Bureau membership logo. PCI consists of a framework of

12 requirements, which are driven by the number and type of transactions that an individual entity stores, processes or transmits. So how are companies actually living up to the PCI/CISP requirement implemented in June 2001. Visa has indicated that out of the 299

entities identified that need to meet the requirement 167 have been verified, 21 received remediation 68 are still in process and 43 are still pending. All service providers were expected to have achieved validation by September 30, 2004.

Special points of interest:

- Over 6,500 in attendance at Defcon (the hacker convention) this year!
- Free Investigators Resources! Visit tcbconsultingonline.com
- Mail Fraud Statute still effective for prosecutions of frauds

United states postal inspectors provide another avenue for prosecution



We all know how frustrating it can be when your company experiences a fraud, you have identified the suspect but you are having a struggle finding anyone that will take the case for prosecution. Did you know that the Mail Fraud Statute is the oldest and the most effective consumer protection law, and the U.S. Postal Inspection Service is the federal law enforcement agency that uses it to the maximum effect. Since the White House named the U.S. Postal Inspection Service a member of its Corporate Fraud Task Force in July 2002, Postal Inspectors have been increasingly involved in corporate investigations, which have been noted by former U.S. Attorney General John Ashcroft as among the most significant

issues facing our nation and our economy. Postal Inspectors aggressively pursue and stop those responsible for Corporate fraud. In addition, the internet is teeming with fraudulent schemes, and swindlers use a variety of methods to exploit people online. Fraud on the internet often results in mail fraud, as "cyber scammers" use the mail to receive payments and ship items. The Postal Inspection Service actively participates in the Internet Crime Complaint Center (www.ifcc.gov). The Criminal Statistics for 2005 indicated that out of 12,073 Arrests the Postal Inspectors obtained convictions on 9486. Mail fraud, Financial Investigations and Child exploitation (cyber crimes) accounted for 18% of the total crimes. The Postal Inspectors enforce more than 200 federal laws in investigations of crimes.

Electronic Crimes (18 USC 1029,1030,1037,1343,2701)

Inspectors protect postal customers from fraud schemes and other crimes that may occur online and involve the misuse of the mail or the Postal Service.



This included using or selling stolen or counterfeit access devices, such as credit card numbers; using protected computers without proper authority or exceeding authorized access; using computer communications in a scheme to defraud using a false identity when sending commercial e-mails to mislead or deceive recipients, as with spam; and unauthorized access to communications that are stored electronically via a communications service....You can access our Website to identify which Inspection Division you need to contact at www.tcbconsultingonline.com.

Expanding Your Relationship with Your Merchant Through Other Risk Channels

Credit cards aren't the only risks that your merchants face in the course of their business. If your merchant is open for business, most likely he deals in some sort of currency. About the New Color of Money: Safer, Smarter, More Secure The new Color of Money will be safer, smarter and more secure. New money designs have been issued as part of an ongoing effort to stay ahead of counterfeiting and to protect the



economy and the hard earned money of U.S. currency users. The first not of the new currency designs, the \$20 note, was issued October 9th, 2003. The series continued with the \$50 note issued on September 28th 2004. The

next denomination was the \$10 note delivered in 2005. The \$100 note is slated for redesign as well. The government has no plans to redesign the \$5 note at this time, and the \$1 and \$2 notes will not be redesigned. Were you aware that you can request media and marketing materials that you can forward to your merchants or post on your web site? Go to WWW.moneyfactory.com/newmoney

Mac's 6th Annual Meeting Held in Seattle

The Merchants Acquirers Committee held it's sixth annual meeting this year in Seattle Washington. As usual it was a full day of sharing information amongst the risk arena of the industry. There were speakers from the Associations, from law enforcement and several vendors that offered different solutions to the challenges that face us all. The MAC directors provided the details of the upcoming incorporation as well as their partnership with the ETA (electronic transactions Association) and the IAFCI (International Association

of Financial Crimes Investigations). MAC is still in the process of trying to partner with the MRC (Merchants Risk Council). The main message that was being presented is that MAC has grown and is a well know resource for Risk assistance and education in the payment industry. MAC is comprised of Acquiring Financial Institutions, Gateway Providers, Internet Service Providers, ISO/MSPs, Merchant Acquirer, Processors, Law Enforcement and other risk management and underwriting



professionals is you would like more information on how to become a member of MAC Access our website at: TCBCONSULTINGONLINE.COM to fill out a membership application.

Take Charge Business Consulting is here to stay!



TCB Consulting was founded early this year by seasoned risk veteran Laurie LeBoeuf. Her expertise in both issuing and acquiring credit card risk surpasses most in the industry. With the market trends now more geared toward the buying and selling portfolios, Laurie saw a huge need within the industry for experienced Risk consultants. The field is so specialized, there are not enough experienced Risk personnel to go around.

Our Risk Specialists have more than 20 years of acquiring operations and risk, 10 years issuing operations and risk, and 6 years in retail loss prevention combined experience. Our team is dedicated to networking and keeping current with issues concerning the credit card industry.

Though we are very involved with law enforcement, our philosophy is much different. Primarily, government

agencies are typically 3 to 5 years behind what is actually going on in our industry. Our specialists are in-tune with what is going on right now. We are able to do this through networking not only with members of the investigations community, but through contact with the darker side of the internet.

The TCB Consulting team members are active in several groups of interest:

- Merchant Acquirers Committee (National Board)
- International Association of Financial Crimes Investigators (National and Local Boards)
- Houston Metropolitan Criminal Investigators Association
- Electronic Transactions Association Member - We are also on the Risk & Fraud Committees
- US Secret Service Operation Direct

Action Task Force (Private Sector)

- US Secret Service HITEC Task Force (Private Sector)
- Credit Card Fraud Investigators Association
- Communications Fraud Control Association

Our team is extremely sales oriented. Competition is huge in our industry and though risk is a concern, retaining your merchants and sales channels is much more important. TCB knows that risk can be done effectively while retaining high customer service standards through good communication and education.

Defcon 14 Update

There is something to be said for one who knows the enemy. One way to keep up with current fraud trends is to attend the country's largest hackers convention. Yes, you heard it right. Hackers gather annually to compare "how to" notes just like we do.

There are many hacker gatherings—Black Hat, Not A Con, Shmoo Con, PhreakNic X, and SyScan to name a few. Defcon is by far the largest. It is a sad fact that approximately 6,500 gathered at Defcon 14 this year, but under 1,000 were in attendance at the International Association for Financial Crimes Investigators. Can we admit we are really outnumbered?

Many industries (usually technology related and federal law enforcement) have gotten wiser and have begun sending staff to Defcon, however the acquiring and banking industries in general continue to ignore the calling.

One of the more entertaining games at Defcon is "Spot the Fed." Participants pull individuals thought to be federal law enforcement agents out of the crowd. If



they find one, the winner gets a T Shirt. Speeches at Defcon include everything from lock picking and safe cracking to psychology and hacking. Some of the highlights from this year's con were:

- Security Law—Delivered by an attorney specializing in electronic crimes.
- Bumping—A session on lock picking which included a demo on bumping open US Post Office boxes and how to make bump keys.
- Metamorphic Software—Viruses which mutate to avoid being picked up by anti-virus software or "increasing genetic diversity."
- Kiosk Hacking
- Smart Card Hacking on Kinkos Cards
- Corporate Network Spying
- Psychology Behind Phishing— Stats on the most effective techniques.
- War Driving—Detecting and mapping open wireless networks.
- Mobile Device Attacks—Blackberries and smart phones.
- Neuro-Linguistic Programming and

concepts of interrogation

One of the more interesting things about Defcon is the psychology junkies which attend. Many of these guys are not IT guys by trade. Many have degrees in psychology. The lecture on the psychology behind phishing was particularly interesting. One of the big points was to target US financial institutions. Below is a slide from the presentation.

Phishing Tip

Target US financial institutions

- They have the worst online security practices of any banks
 - Users are largely ambivalent towards adopting these poor security practices.
- Second worst are UK banks
- Second best are Australian banks
- Best are European banks
 - PIN calculators, smart cards, TANs (one-time per transaction PINs), ...
 - Don't bother with these unless you really know what you're doing

It is overwhelmingly disappointing not to see anyone from the acquiring industry at the conference each year. Hopefully financial institutions will wake up and start sending more people. Understanding your enemy is key in risk!

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

Phone: (281) 797-9044
E-mail: lleboeuf@tcbconsultingonline.com

***Delivering significant and measurable
results!***

We're on the web!
tcbconsultingonline.com

New resource for investigators

Take Charge Business Consulting, LLC has collected a huge number of investigative sites which we update upon request. The site is maintained and is accessible to anyone who wishes to use it...free of charge!

We encourage you to give it out to your investigators! The site includes links for the following types of research:

- Skip Tracing (People, emails, phone numbers, etc.)
- Public Records
- Site Inspection Resources
- Government Agencies
- Commercial Mail Receiving Agencies Look Ups
- Package Tracking
- Networking Groups
- Whois Searches
- Tracing Software

- Research by Business Types
- Criminal Justice
- Legal
- Hacker Sites
- International Research
- Non Profit Research

We are expanding the site daily and we love to hear feedback!

www.tcbconsultingonline.com

Click on Investigators Links!



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.