

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 5
September 3, 2008

New id reader validates state issued ids for all 50 states-rapid compliance solution-red flag rules!

SNARE is a new system on the market used for validating state issued pieces of identification. It was designed with the new Red Flag Rules in mind.

This system is an inexpensive and rapid implementation piece for financial institutions, hospitals, car dealerships, cell phone providers, check cashing, and large ticket merchants to name a few.

The premise is simple. There are literally 2 million websites selling fake pieces of identification. Many are so good, even a trained member of law enforcement cannot detect it by just looking at

them. Not many (if any) people can validate identification pieces for all 50 states.

Most fake IDs are not properly encoded on the magnetic stripe or the 2D Barcodes. This system allows the user to swipe the ID piece. The system validates the algorithm on the barcode or magnetic stripe, then displays the information on the screen to allow comparison to the ID piece.

The readers tie to a database which allows multiple locations/branches see how many times that id piece has been used.

The system also houses an alerts system which allows an identification piece to be tied to an account number. If an account number has been deemed fraud or an "at risk" account, the next person presenting the identification piece will flag with an alert.
Con't on Page 5.



the Take Charge Challenge—Reduce your losses-no consulting fees!

TCB is excited to announce that we are ditching consulting fees for portfolio loss evaluations. If you think your losses are too high, TCB will perform a loss analysis for zero dollars in consulting fees. Our fees will be calculated as a percentage of what we save you over 6 months. If TCB does not take your losses down, we do not get paid.

This bold move is saving the industry thousands in both credit and fraud losses. TCB is predicting more and more in out of business losses. If you are being affected by these

and/or other types of losses, TCB can help.

In most cases the audit is performed offsite which means no travel expenses. We review policies, procedures, system parameters, and interviews with key staff members.

We take into account the size of your business, portfolio mix, and business philosophy. Your recommendations will be tailored to your business for rapid implementation and customer service toward your sales force will remain a top priority.

Risk Counseling Service Hotline Is Launched

TCB has launched a risk counseling service hotline. This service allows an ISO/processor/bank to retain TCB 24/7 to answer questions on compliance, underwriting, and risk, help handle emergency money recovery, provide advice during a crisis, and work through training issues.

This service is perfect for start up departments, new ISOs, ISOs assuming their own risk, ISOs taking on a new type of risk, and new compliance, underwriting and risk employees. For more information about subscribing to this service, email service@tcbconsulting-online.com or call 713-822-4368.



Special points of interest:

- New Identification Reader—ID Validation for All 50 States
- Portfolio Loss Evaluations—No Consulting Fees
- Risk Counseling Service Hotline is Now Available
- Microbilt Credit Products
- High Risk Site Inspections
- Defcon 16 Review
- When to Ask for a Subpoena
- Case Template for Submitting Cases to Law Enforcement
- Medeco High Security Locks—Check your doors!
- Red Flag Rules
- TCB Website Updates

Microbilt

TCB tries to review companies and find products helpful to the financial crimes world. Microbilt is a company of interest to anyone extending credit. They offer a huge variety of services including business credit reports, bankruptcy indicators, collections, site surveys, interfaces between the credit bureaus and internal boarding systems to name a few.

The credit bureau interface to internal boarding systems is one of the most useful. Programming time is cut considerably because the interfaces are already written. The user just defines what data they want imported back for print or storage within their system. The users can even customize scoring features.

Micromerge is an interesting tool. Microbilt takes all 3 credit bureaus and merges the data so that the user can get a complete picture of the individual's credit.

The business reports are user friendly and easy to read. Trending in some of the reports are good indicators of upcoming

bankruptcies.

Microbilt's collection services include skip tracing, credit reporting, and letter generation for internal collections. If internal collections doesn't fit the need, users can even outsource collection items through their system. The system also allows users to add unpaid balances to the bureaus.

Microbilt offers an online interface with all of the usual searches for credit bureau reports, criminal history, people searches, OFAC, and asset searches.

Microbilt also publishes a free newsletter called "See" which includes informative information about compliance, laws, new products, etc. You can sign up for the newsletter on their website: <http://www.microbilt.com>.

For more information about any of the Microbilt products, contact Jason Skelton at 800-375-7324.



High risk Site Surveys

TCB is in the process of forming a high risk site survey team. This team consists of experienced fraud investigators throughout the U.S. Traditional site survey companies will drive by and snap pictures. This project is designed to act as an extension of the risk department.

The investigators will be briefed on the case then go to the location, question individuals, attempt to recover sales drafts, and gather important data from the location.

This service is in beta testing but is rapidly growing as we add qualified individuals to the team. Currently, there will be some areas not easily covered due to the experience requirements needed for these inspections. We can always fly an investigator out to a site.

If you are an investigator with at least 5 years of fraud experience and would like to earn extra money performing high risk site surveys, please contact Deana Sellens at dsellens@tcbconsultingonline.com or call 713-822-4368.

DEFCON 16 A review on the hacker's conference



Defcon 16 was extremely informative

this year. For those of you who did not go, Defcon is a hackers convention. Over 8,500 attendees showed up to listen to the latest and greatest security flaws from around the world. This by far was the best group of speakers we have seen over the years. Kudos to the Dark Tangent!

The experience is one of a kind. Attendees can watch and learn best practices for physical and computer security from some of your best adversaries and other security specialists. They learn all forms and concepts of lock picking, safe cracking, the newest breakthroughs in computer security issues, and hardware hacking.

Why send your loss prevention and IT security people? Here are just a few of the highlights of interest for the financial crimes world.

- Medical ID Theft
- Compromising Networks Through IT
- Satellite Feed Monitoring
- Smart Cards
- Unique Creds

- RFID Hacks
- Death of Cash

The issue of medical identity theft is huge. There is a widespread problem with security in hospitals centered around the public areas in hospitals and wireless networks. There are issues with patching due to the wide range of equipment attaching to these networks and lack of anti-virus software on these networks. Most think medical identity theft only effects the insurance companies. What if someone stole your identity to receive treatment and it caused erroneous information to show up on your medical profile? Hospitals store more than enough data to take over your financial identity.

Another interesting talk was that security companies are tending to find that corporate networks are much tighter now and more difficult to penetrate via the users. One security company says they are actually having more luck in breaking in through IT staffers' computers. The majority of the vulnerabilities they are finding are through the browsers, Acrobat, Office, and mail clients. They are using tools such as Metasploit, Core

IMPACT, and other "hostile attack tools." This brings up the point of who is watching the watchers at your company?

One of the most interesting subjects was about satellite feed monitoring. Many of the processors and major banks use satellite feeds to transmit data. There is a whole following of geeks who monitor these feeds. Many just use it to watch free pay television, but many read email and review data files. Feedhunter.com is an interesting site. He has captured several images from satellites he is watching.

The Smart Card hacks were interesting to watch. The presenter discussed the different physical layers of smart cards and how to bypass each with a microscope, needles, and low voltage electricity. The presentation was interactive with live demonstrations cracking into, reading, and modifying these cards.

The discussion on unique credentials demonstrated how to mold body parts to bypass some biometric identification security and scanning for RFID credentials people may be carrying. The conference always features the beloved "Wall of

Continued on Page 4

Subpoena or no subpoena...that is the question

Over and over again I get the question as to when a subpoena is actually necessary. Where does your company stand?

Scenario 1:

Company/Bank is called by a member of law enforcement because another company fell victim to a fraud scheme. If you are not a victim, you should always ask for a subpoena. As a general rule of thumb, if you did not suffer a loss or have some type of evidence of your own that an account was set up fraudulently, then you should ask for a subpoena.

Scenario 2:

Company/bank suffers a loss. Company/bank calls law enforcement for help. Company/bank refuses to provide law enforcement with any documentation about the crime without a subpoena. Company/bank gets upset because law enforcement doesn't arrest anyone.

This issue comes up constantly. Come on guys! First of all privacy issues do not apply if you are a victim of a crime. You can lawfully report a crime without a subpoena if you are the victim.

The attorneys will always tell the company to get the subpoena because they are attorneys. An attorney is there for advice, not to tell you how to run your business. How many banks actually get sued by an inmate?

If you are not prosecuting cases because you will not work with the police to get them the evidence of the crime you are a victim of, shame on you.

TCB works with law enforcement on a regular basis and I am still amazed at the number of companies and banks who are victims and will not help out law enforcement.

Law enforcement has to overcome so many hurdles as is. If you are preventing the apprehension and arrest of criminals because of red tape created by your own attorneys, you really should sit down with the powers at be and rethink your policies.

Help law enforcement help you. Remember, the crooks will go after the banks who are not getting arrests.

Creating a Case template—submitting cases to law Enforcement for prosecution

Many companies use the excuse that filing a police report is too much work and not enough manpower. Developing a case template is extremely important in streamlining the process and making the job easier for law enforcement.

In a perfect world, every member of law enforcement can focus 100% of their time to your case. Unfortunately, law enforcement is stretched to the max. Your case will get worked much faster if it is well organized and easy to understand. You can always hire TCB to work your cases, but if you don't have that luxury, take a day to organize a case template that will work for you.

TCB has prepared some sample documents which are posted on our website. Some are geared for the acquiring industry and some are more generic. If you have a good sample template for another industry that you would like to share with everyone, send it to webmaster@tcbconsultingonline.com and we will post it.

A case template should include the following:

- **Investigator's Checklist**—This checklist should be a guide to remind the investigator of all of the things they need to do after a fraud has been identified. When a fraud occurs, it is important that everything is covered quickly. Fumbling around and haphazardly working pieces will cost you valuable time and money.
- **A cover letter** explaining the ins and outs of what your company does and how your systems work. This information will not change, so have the cover letter started. For example, the merchant acquiring industry is an enigma to a lot of people. Explain what an acquirer does, how the money moves, and then go into a section of how the fraud was committed. Detail the fraud in a step by step account with names, dates and account numbers. Mark each section with Exhibits referencing your pieces of evidence. This cover letter can later be used for your narrative on the SAR. Remember to lose the abbreviations and industry slang—SPEAK ENGLISH! Cops don't do your job. Could you decipher all of the radio number codes law enforcement uses when speaking to each other? "Fellas, we got a 918!" It's the same thing in reverse.
- **Exhibits**—Pull and label each screen shot, application, credit bureau, etc. that brought you to the conclusion of fraud has been committed. Place each in order behind the cover letter. If the case has any account numbers of any kind associated with the fraud where you cannot access the data, make sure you include the contact information on each account. For example, if I was reporting a fraud where 100 card numbers were used, I would run a report with the card number and each issuer with the bank name, contact phone number to the fraud department, and subpoena address by each card number. Build these types of queries and reports in advance, so you are not scrambling to look them up.
- **A Custodian of Records Affidavit**—This document is required in about every state. Include it up front with your documentation. This will keep you from having to send a second copy of everything at a later date. This form is notarized and basically states that all of the documents are legitimate and came from your company.

Law enforcement will ask for every one of these things. If you get them submitted where your case makes sense, your case will get worked faster. If law enforcement has to stop and keep calling you for more information, you will not see progress. Here are a few more documents you should keep on hand and ready in case you need them:

- **Suspicious Activity Report (SAR)** - All financial institutions should be filing SARs with their back end banks on any suspicious activity whether or not there was a loss.
- **Hold Harmless**—This allows your investigators to work with receiving banks to freeze funds. It takes the liability off of the bank and puts it on your company. Most banks will not freeze funds and send them back to you without one of these.
- **Affidavit of Fraud and Forgery**—This document should be signed by anyone claiming to be a victim of identity theft. The FTC's website always has one available that most banks will accept.

We hope this information will help you prepare a good template and make your cases a little easier to turn over.



Medeco high security locks



Marc Webber Tobias spoke at Defcon on the new found security flaws in the Medeco High Security Locks. The lecture was frightening due to the ease of entry into these locks.

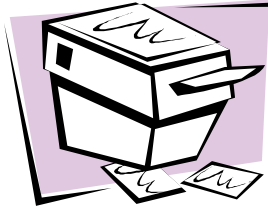
Tobias is the author of the book [The Compromise of Medeco High Security Locks: New Techniques of Forced, Covert, and Surreptitious Entry](#). He runs a website called Security.org. Tobias is an attorney who specializes in technology cases and they have security laboratories who research various methods of forced and covert entry.

Tobias performed live demonstrations of the security vulnerabilities using a paperclip, a screwdriver, and a flat blank key cut from various materials spanning from cardboard to credit cards.

He stated that Medeco is saying that there are no guarantees for locks due to new developments in lock-picking techniques. Medeco represents about 70% of the locks used in commercial and government entities in the United States.

Tobias demonstrated 3 critical flaws in the

security of these locks. One of which is key control. He coined a new phrase, "KEYMAIL" which refers to the emailing or faxing of a copy of a key. A new key is then made with the copy through various fashions which include scissors, exacto knives, key cutters, etc.



The other 2 major flaws were forced and covert/surreptitious techniques. Medeco locks were thought to be bump-proof, however Tobias demonstrated that the locks can be bumped.

For those who are not familiar with bumping, it is a technique where a blank is fashioned into a generic key. Without getting too technical, keys are made with specific dimensions. There is a certain amount of space between the hills and valleys on the key. The attacker makes the hills the tallest and the valleys the lowest. The key is then inserted in the lock and then you tap it with a small

hammer until the key turns. It is called bumping because of the tapping used to gain entry. The high security locks have a little more involved when bumping them open, but someone can still gain access in under 30 seconds.

Tobias spoke on bumping open US Post Office boxes 2 years ago. The Postal bump keys open any post office box. These bump keys can be purchased over the internet.

Tobias also managed to reverse engineer the codes used to cut the keys and found that he could open any lock with only a set of 4 master keys.

This article is very basic, for more information on the Medeco security flaws, Please visit Security.org.

Tobias will be speaking at the IAFCI Gulf Coast Chapter meeting on September 18th. If you are currently using Medeco High Security Locks to secure your assets, you may want to attend the conference. His book can also be purchased on his website.



A Review of Defcon 16 Continued from Page 2

Sheep." The Wall of Sheep lists the IDs and passwords of anyone logging into the wireless network who didn't have enough security on their pc. The RFID carriers may be on the Wall of Sheep next year with the person's picture. RFID is used in security badges, some Visa and MasterCards, passports issued after late 2006, bus passes, etc. If you are carrying one of these pieces of identification, they will sniff the piece of identification and then post your picture on the wall with data from your identification piece.

Another presenter showed a demo on a scanner that penetrates the RFID reader and cracks the codes to allow access. The scanner can also kill/"zap" the terminals and counterfeit the identification piece. The case study was performed on the Amsterdam subway system.

The discussion on the death of cash went into details as to what banks and the government monitors concerning cash transactions and why credit cards are a bad thing. He gave examples of DoS (Denial of Service) and other types of outages on banks are strong reasons to keep cash alive.

It looks like the International Conference for the International Association for Financial Crimes Investigators will had roughly 800 attendees this year. I find this quite sad considering the Defcon had over 8,500+ in attendance. Companies should really think about this when they are budgeting for training for IT Security and Loss Prevention Personnel. Your security people are severely outnumbered. Everyone is always in a reactive mode rather than taking proactive measures.

Exposure to conferences like Defcon gives your security people a different outlook on how the world really works while conferences like the IAFCI gives them the contacts they need to network with and survive. Can you afford not to send your staff? For more information on Defcon, you can visit their website at www.Defcon.org. We hope to see you at Number 17!

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.

SNARE—NEW IDENTIFICATION VERIFICATION READER ON THE MARKET CONTINUED FROM PAGE 1

The database can be hosted on an internal or web server, so the entity is not relying on yet another third party provider's security for sensitive data. Once implemented, the entity must simply integrate the use into the policy and procedure manuals and they have achieved compliance with the Red Flag Regulations.

The system is also capable of functioning as a stand alone pc. This situation is ideal for a single check cashing, a merchant taking checks for high dollar tickets or performing financing of any kind, etc.

The units (valued at \$450 each) are supplied at no cost to anyone signing a 3 year service and licensing agreement. This product is ideal for resale. ISOs, processors and MSPs can become resellers of the SNARE product.

Initial studies show a 95% reduction in the use of fake pieces of identification after implementation of the SNARE system.

If you would like to learn more about the SNARE product or see a demo, email Service@TCBConsultingOnline.com to schedule an appointment.

For more information about the Red Flag Regulations, see the article below.

Red Flag Rules

The latest buzz in the financial world is new Red Flags Rules which should be in place for financial institutions by November of this year.

In a nutshell, the FTC/federal government is requiring financial institutions to put identity theft prevention measures in place when opening new accounts and monitoring existing accounts. There are 3 basic items which must be addressed:

1. The entity must have and maintain/update reasonable procedures for detecting, preventing and mitigating identity theft.
2. The entity must be able to identify relevant patterns of activity signaling possible identity theft.
3. The entity must incorporate the detection of patterns signaling identity theft into their policies and procedures.

The term financial institutions leaves the scope wide open. TCB verified with the FTC and basically anyone signing up accounts where money is going to be moving around is considered a financial institution. This applies to ISOs, banks, processors, check cashing,

payday loans, and cash advance companies to name a few. Car rental/leasing companies, auto dealerships, cell phone providers, hospitals, and anyone else extending credit also falls within this realm.

Many smaller businesses do not know that they are being impacted by these new laws. If you do business with any of these business types, mention the subject to them. Education is key.

The challenge for everyone is that some transactions require a more in depth look at the person while others do not. Keeping the lines moving at a bank teller window is important, but the person's identity still needs to be established. A bank obviously cannot pull credit on every customer coming in to cash a check.

Banks are having to implement a face to face quick verification process and a verification process for bigger transactions, loans, etc.

If you would like to learn more about the Red Flag Rules and how it might impact your business, you can visit the FTC's website: <http://www.ftc.gov>.

TCB Website Updates

We have added some cool and groovy new pieces to our website. Of course, it's free for everyone!

INVESTIGATORS TOOLS—This page features forms and documents frequently needed for investigations.

READING LIST—A list of suggested reading for investigators.

TRAINING OPPORTUNITIES—Seminars and educational workshops for our industry. Non profits and law enforcement can post to this page. Just email the information to us.

PREFERRED VENDORS—This is a list of vendors that TCB has kicked tires and test driven. These are not paid ads.

GOOGLE SEARCH ON THE INVESTIGATORS LINKS PAGE—We added a Google search to this page so investigators can set it to their home page.

The Investigators Tools and Links are only as good as we make it. Please feel free to contribute comments and information. Remember, our specialty is credit cards. We really love input from all types of fraud industries. We read all email and appreciate the networking!

United we stand!

Advertising Space Now Available in the Acquiring Mind!

Quarter, Half, & Full Page Ads Now Available

Reach thousands of industry professionals

Ads starting as low as \$50 an issue

*Law enforcement and industry non profit organizations advertise conferences and seminars for free.**

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

**Dependent on availability of space. Some restrictions may apply.*



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!

Are you environmentally friendly? To subscribe to this free newsletter electronically and ditch the paper, please visit our website:
www.TCBConsultingOnline.com/Publications.htm



STOP FRAUD NOW!

Deadline for Red Flag Program is November 1, 2008

SNARE stops identity theft and fraud by:

Authenticating State Issued Photo Identification Pieces Real Time

Creating a Communication System Between Multiple Branches/Locations

Managing Alerts Real Time

This system takes care of 2 of the 3 red flags you need to cover for compliance! The third is simply incorporating SNARE into your existing policies and procedures.

A single installation for as little as \$200.00 per month. Optional reader hardware is provided at no charge with 3 year contract. (\$450 Value)

For more information, call (281) 719-8591.



MSP in a Box

Web-based Software Solutions to Fit Any Operational Need

The EZ Enterprise suite of products ("MSP-In-A-Box") allows an ISO or MSP to automate and manage all facets of their business from anywhere in the world. Use one or all components. Host in house or with ePayware. EZ Enterprise is so flexible, we can accommodate any operational and budgetary need!

- u EZBOARD (Boarding and Underwriting)
- u EZMERCHANT PORTAL (Transaction Monitoring)
- u EZRISK (Risk Management)
- u EZTELEMARKETING (Lead Generation/Distribution)
- u EZPAY PORTAL (Commissions and Residuals)
- u EZLEADS (Lead/Sales Management)
- u EZENROLL (Application Processing)
- u EZPOS (Terminal File Build Automation)
- u EZSHIP (Asset Management)
- u EZCSR (Customer Issue Tracking)



Lower Costs, Drive Revenues, Mitigate Risk

Contact Ray Somani: Ray@epayware.net or (408) 417-0123

www.ePayware.net