



▶ CHARITABLE TRUSTS: GATEWAY TO ANTI-MONEY LAUNDERING 1



▶ BEWARE OF HIGH CHARGEBACK MERCHANTS! 2



▶ PUZZLE TIME 4

risQVu

TECHNOLOGY & FRAUD RISK IN BANKS

2012: The Year of 'Fraud Control' !

The year 2011 has witnessed some very interesting frauds across industries. Fraudsters have been outwitting the fraud controls time and again.



Polymorphic nature of fraud is quite evident. Advance persistent Threat (APT) is one of the major modus-operandi for bigger crimes. In APT the attack objectives typically extend beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and initial goals reached.

There is another noteworthy development on fraud control which happened across the globe is banking regulators across the globe mandating "Multi layer controls" to combat frauds. These multilayer controls interalia include, Risk Based Authentication, Behavior based Fraud Monitoring solution, Setting up of Fraud Risk Management Framework.

Thus the year 2012 is expected to be year of "Fraud control". Many organizations, specially Banking and financial services companies will go for setting up of an intelligent Fraud risk management framework and also will implement smart solutions to combat frauds. But Fraudsters will also not sit silently. They will always try to innovate and outwit controls But RisqVU is committed to chase them and bring the readers the latest solutions to outwit the fraudsters!

- D P Dube

Charitable Trusts: Gateway to Anti-money Laundering

Money Laundering is the process of concealing financial transactions to make illegitimate money appear legitimate especially earned through various illegal means; to name few:

- Illegal gambling
- Terrorism
- Embezzlement
- Corruption

The basic idea or objective is to hide the true source of illegal proceeds and make them appear legally usable by transforming these illegitimate earnings to legitimate via various financial transactions.



Today's fast growing technological sector has simplified & has assisted these money launderers to adopt innovative means of transferring their illegitimate funds quickly anytime & anywhere which in return has been a challenge for the legal authorities to identify & action them.

Though such transactions at a very later stage is noticed by the respective authorities but the action hit rate currently is still insufficient to stop them at an ab-initio stage.

Reasons why Charitable Trusts are conducive for AML:

Instances where a fraudster has stolen, skimmed, counterfeit etc card (Domestic/ International) can be swiped at EDC machine or can be used online for donating to a charitable trust, and this type of fraud creates direct cash liquidity. This is more conducive practice for a fraudster because tracing him becomes difficult

as no good/ service is made available under such MCC which would assist during investigation in identifying his crime.

Since Charitable Trusts are open invitations for

putting money which remains undercover & unquestioned when investigated for usage; following steps should be taken to prevent money laundering:

- Acquirers should use automated Anomaly detection system for monitoring cash inflow of transactions
- The anomaly detection system should be able to detect all

sorts of merchant acquisition fraud

- Site Verification & KYC should be very elaborative
- Subject to the set up & type of charity services an upper limit as to the total amount of the transaction that has happened in a particular day, week or month should be designed
- Acquirers should insist for domestic cards acceptance for the charitable trusts since all Issuers within Indian geography are 3D secured hence both CB & Fraud loss will be nil or controllable.
- Monitoring the cash inflow in cases where FCRA accounts are available
- Monitoring Card usage with all permutations & combinations

[The purpose of this article is ONLY to convey to the readers the controls required to prevent /detect acceptance of illegal deposits through various means]

Beware of High Chargeback Merchants!

A chargeback (CB) is the reversal of a previous sales transaction which occurs when a card holder disputes a specific transaction(s).

Monitoring or reviewing merchants highlighted under high Chargeback is important for two foremost reasons. **Firstly**, if the merchant himself is involved into fraudulent activity or he has been targeted by the fraudsters. **Secondly**, fraud loss or penalty from Associations which directly effects the revenue of an acquirer along with ruined goodwill & market position as an Acquirer.

Below are the few areas which should hint the acquirers that merchant is involved in initiating fraud:

- During chargeback presentation, requested information by the acquirer i.e. bill copy, receipt was found illegible or missing
- Actual transaction amount debited to customer was found different when compared with receipt or the bill copy
- Duplicate Processing/ Processing Error: Merchant processed an incorrect transaction amount, merchant processed card number that did not match with that of transaction receipts, transaction receipt was altered without prior knowledge of cardholder
- Authorization of transaction was declined by the gateway but merchant completed the transaction manually
- Reoccurrence of chargeback(s) on same merchant
- Peer grouping of merchants to find out the link among them with different attributes; Multi dimensional profiling of customer (card No) & the merchant

- Non- Receipt of Product/ Service when the merchant had taken the payment from cardholders account but the requested product or service was not delivered
- Cancellation of recurring transaction (Monthly, Half yearly, Yearly): Though customer has canceled his services with the merchant but still cardholder is being debited for such services or goods with non-delivery of the same i.e. where transaction exceeded the amount assigned to terminal

To overcome future losses occurring from such CBs, acquirer should practice:

- Fortnightly review the merchants transactions & type of chargeback being reported
- Merchant training for more than one chargeback report
- Modify the payment cycle to 3 Day Delay Funding (DDF), 7 DDF etc which ensures to pool some liquidity with acquirer for future chargeback(s)
- Initiating temporary blocking of BIN which have contributed to high fraud chargeback on the merchant
- Policy on the web page (in case of e-commerce merchant) should be clear enough to educate customer
- Develop controls to avoid duplicate processing
- Analyze average transaction to that of chargeback that has been reported on each MID, TID of merchant i.e CTS ratio
- Establishing txn control & velocity limits
- Profiling of the merchant & customer to identify the anomaly.

Intelligent Customer Interaction Technology

New era banking enhances the communication between customer and Bank. Using automated intelligence and customer data profiles, personalized support is delivered in the customer's preferred communication channel – web, mobile, SMS, or telephone.

Integration with existing banking systems helps identify the root cause of arising issues, giving customers the information and action they want.

Integration with existing banking systems helps identify the root cause of arising issues, giving customers the information and action they want..

This intellect between Bank and customer is Digital Banking, which supports multilingual interface via **Voice, Free Text and Tap/click**. The system selects and populates each dialog using a **personalized** decision process. Solution inhibits self-learning based on **customer data, historical service log, cases that are processed by the system** and can seamlessly integrates with a human operator to get advice behind the scenes or complete transfer to solve problematic cases.

US Based, Personetics has Digital Bankers resolution in this space.

Debit Card Fraud at an Indian Bank

A Software engineer based in Pune, India received two SMSs mentioning that her XYZ debit card was used for purchase worth Rs 93,000 and Rs 5,000 (Approx 2000\$). Upon contacting the Bank's customer care, she was informed her debit card was used to make online purchases. Subsequently the card was blocked to avoid further misuse. It is suspected that fraudsters might have hacked the details of debit cards to make online shopping or have used cloned cards to make purchases.

Debit cards can be stripped by a fraudster using a special scanner that collects the digital information from the card. The owner of the card has no idea that their information has been compromised. Often, debit card scanners are installed on ATMs and are virtually undetectable. A camera or magnetic device set up nearby captures the PIN entered by the victim. The victim is unaware his information has been compromised until he notices strange purchases made on his account.

Gift cards, similar to debit cards, are even more attractive to fraudsters because they contain no customer information. They're just like cash. One of the most common gift card scams is when a fraudster takes a pile of gift cards off a shelf in a store, sneaks off to an isolated spot, and then uses a scanning device to capture the identifying information contained on gift cards -- all without ever leaving the store.

Source: <http://news.oneindia.in> and www.acfe.com

RBI or Reserve Bank of India (the Central Bank for India) Recommends Card NOT Present Transaction (CNP) Guidelines

All types of card business carry fraud risk of extreme nature due to the kind of global exposure card transactions face, whether CNP or Card Present transactions.

Last year, during June 2011, the working group on securing card present transactions, appointed as per RBI memorandum, released guidelines on required controls for fraud prevention. In this article, we'll take some of the key recommendations and try to understand how they can help in fraud prevention and how they can be set in place as well.

- All Acquirers and Issuers may put in place adequate fraud risk management systems and processes

Acquirers and Issuers – both are required to have adequate FRM systems. These two are different requirements from various aspects. The profiles that can be created at acquirer's place carry extremely valuable information about each merchant and can help in detecting the fraudulent merchant to begin with.



However, the profiles at the issuer's data repository are mostly about how a particular customer is behaving and can help us know the deviation from her normal behavior. To settle the disputes and hold the right weak link responsible, we need fraud monitoring at not only issuer's place but also at acquirer's place.

On top of this, there should also be a mechanism through which correlation can be done between the profile related information at both the ends. Merchant's information can be linked with the customer's information and collusion can be detected if any. This can provide significant value to the card and banking industry and can help further in fraud prevention.

- Fraud mitigation strategies including all aspects of fraud control viz Detection, Investigation, Deterrence & Prevention and would in-

clude the following:

1. Fraud Detection Capability
2. Transaction & Settlement Monitoring
3. Online SMS Alerts
4. Investigation capability
5. Reporting of Frauds to regulators, franchisee and senior management

Transaction Monitoring is an interesting and most vital piece of the entire fraud management program. The program may have two objectives – prevent losses or prevent frauds. In case the objective is just to prevent loss, the mechanism can be offline detection before the settlement is done between the merchant and the acquirer. This would lead to dispute & settlement management subsequently, however. Settlement monitoring is a key requirement to mitigate risk arising from the merchant locations and can be achieved through offline / near real time monitoring coupled with strong case management features.

A stronger and more ambitious goal is to prevent the frauds in real time. To achieve this, the fraud management solution must be capable of real time integration with the switches at acquirer's place. This will require integration readiness in ISO8583 format. Thus real time ISO8583 based integration becomes one of the key selection criteria for the solution. Organizations should go for those solutions which are capable of integrating and can provide efficient interface to exchange the data in native format. This can help in achieving the targeted response time, which may often be within milliseconds timeframes.

Investigation capability is an outcome of effective monitoring combined with strong case management abilities. Thus the solution should not only respond in time but also provide comprehensive work flow environment which can be customized for organization specific case management requirements.

Rare Legal Fight on Card Company

A part of the payment card industry's powerful but flawed system, securing card data by fining merchants for failing to secure their data, has been taken on by Utah based small celebrity-friendly restaurant.

Stephen and Theodora "Cissy" McComb, owners of Cisero'sRistorante, Utah, have filed a lawsuit against U.S. Bank claiming that the financial institution wrongfully seized about \$10,000 from the McCombs' account to pay \$90,000 in fines. This fine was imposed by Visa and MasterCard alleging that Cisero's had failed to secure its network as per prescribed PCI guidelines and suffered a data breach that resulted in fraudulent charges on customer bank cards.

The unresolved dispute shows that it's just not enough to have PCIDSS recommended preventive controls in place. It's equally important to have detective controls that can read the transactions and interpret the behavior of the possible fraudsters before the fraud can take place such that disputes don't even arise.

Source: <http://www.wired.com/threatlevel/2012/01/pci-lawsuit/>

Cross Channel Fraud Threat to Online and Mobile Banking

With number of consumers using Mobile Banking expected to grow multi fold across the globe, mobile banking has a potential to become the favorite target of fraudsters.

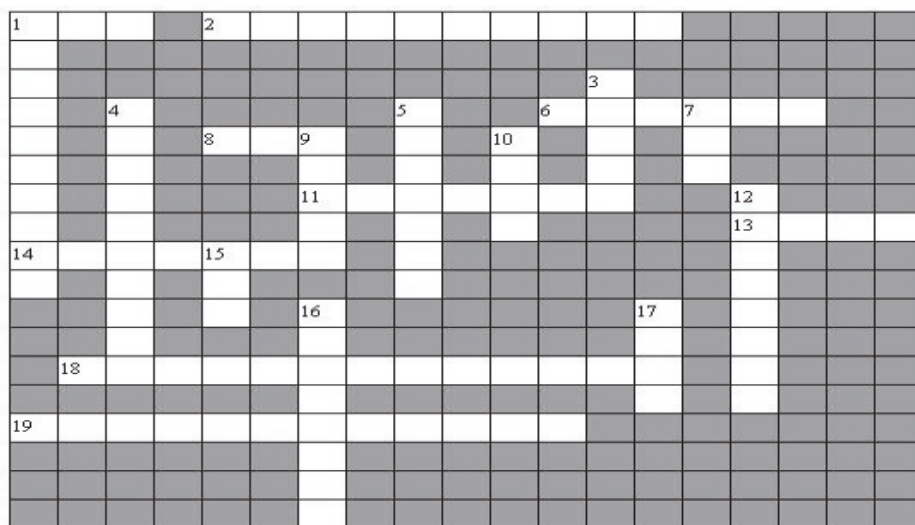
There are two crucial steps required to discourage the fraudsters and prevent frauds – 1) monitor the cross channel fraud patterns that link online and mobile banking systems 2) ensure mobile platforms and services have considered the fraud risk before launch.

Already Trojans such as Zeus and SpyEye have been detected in mobile channel. Recently, attacks are seen on Android that can record the entire voice communication.

Overall, same kinds of threats are expected in Mobile Banking as are seen in Online Banking especially related to electronic payments.

Source: <http://www.bankinfosecurity.com>

Puzzle Time



ACROSS

1. Security on cards has been enhanced recently through ___ as compared to magnetic strip
2. The breach point in a paymnet card fraud on a merchant, processor, etc is known as Point of ___
6. ___ eliminates the need of signature in electronic PoS
8. RBI has granted authorisation to NPCI to take over the operations of ___ in Oct. 2009
11. What is another term for zombie computer army
13. ___ value is a string of characters that represent encrypted data (Computer security term)
14. The mode of accepting payments without real-time connection
18. Someone pretends to be someone else
19. Theft from deposit accounts by way of multiple points of access- whether branch, ATM, Call canter, Debit card, online banking, ACH or wire is known as ___ fraud

DOWN

1. What is the process of encoding information in a way so that only someone with the key can decode it
3. What kind of malware typically resides in larger innocent computer program
4. What is the kind of fraud when frausters asks you to make a payment in return for receiving a substantial amount of money
5. Electronic image of a card on web page or on an e-mail is called ___ card
7. Digital certificates which maps public keys to entities, securely stores these certificates in a central repository, and revokes them if needed
9. A global computer reservation system developed to automate american airlines booking reservations
10. Association that user 4 digit numeric code as CVV
12. A method of online identity theft
15. Triple DES technology algorithm was launched by ___
16. ___ is a mobile phone security attach in which the user is strict into downloading a trojan horse, virus or other malaware onto his phone
17. Fire Brigade Attack also known as ___

Please send your answers at: bfrm@paladion.net
 We will come back to you with your score as well as detailed explanations to these answers.

Offices

INDIA

Bangalore

Shilpa Vidya, 49 1st Main, 3rd Phase
 JP Nagar, Bangalore 560078
 Phone: +91 80 42543444
 Fax: +91 80 41208929

Mumbai

606, A Wing, 6th Floor, Technocity
 Mahapae, Navi Mumbai 400710
 Phone: +91 22 41615151
 Fax: +91 22 41615161

EUROPE

London

CityPoint, 1 Ropemaker Street
 London EC2Y 9HT
 Phone: +44 (0)845 2270777
 Fax: +44 (0)845 2805333

GERMANY

Paladion Networks Limited
 Ahorn Loesungen Deutschland, GmbH,
 Ulmenweg 1,70771, Leinfelden-
 Echterdingen,
 Germany
 Phone: +49 711 7224 9626
 M: +49 176 9680 1738

MIDDLE EAST

Sharjah

Executive Suite, SAIF Zone,
 PO Box 120398, Sharjah
 Phone: +971 50 8344863

Qatar

Paladion Qatar WLL
 P O Box 9584, Doha Qatar
 M: +974 66184607, Fax: +974 44371647

Riyadh

Office # 12, 2nd floor, Sadiri Building,
 End of Jarir Street, Al-Malaz,, Riyadh,
 Saudi Arabia, P O Box 325377,
 Riyadh 11371
 Phone: +966 1 291 0110, Fax: +966 1 477
 6117

MALAYSIA

Kuala Lumpur

Paladion Networks
 F510, Block F, Phileo Damansara 1
 No. 9, Jalan 16/11, 46350
 Petaling JayaSelangor Darul Ehsan
 Phone: +60 3 7660 4988
 Fax: +60 3 7660 4998

USA

Virginia

12801 Worldgate Drive, Suite 500
 Herndon, VA 20170, USA
 Phone: +1 703 8713934, Fax: +1 703
 8713936

CANADA

Toronto

First Canadian Place-Suite 5700
 Toronto, ON M5X 1C7, Canada
 Phone: +1 416 273 5004, Fax: +1 416 273
 1867

Management

CEO: Rajat Mohanty

Editorial

Chief Editor: D. P Dube

Editor: Piyali Guha