INSIGHT

Financial Services Thought paper
Domain Competency Group

QTR 2 2012 – Vol. 2

Frauds in Banking – A perspective

Collabera

Authors:-

Devdatta Rivonkar
Senior Consultant
Domain Competency Group

Ashoka Kumar Palavalli
Senior Consultant
Domain Competency Group

Contents

No part of this document should be reproduced in any form without prior consent of DCG, Collabera
www.collabera.com

Perspective – Frauds in Banking

Executive Summary

Over the time, Banking customers have developed a preference for transacting through newer channels like payments cards and online banking over traditional banking channels. While these payment channels have the advantages of ease and speed of transacting, on the flip side, these very advantages make bank's customers vulnerable to the ploys of fraudsters.

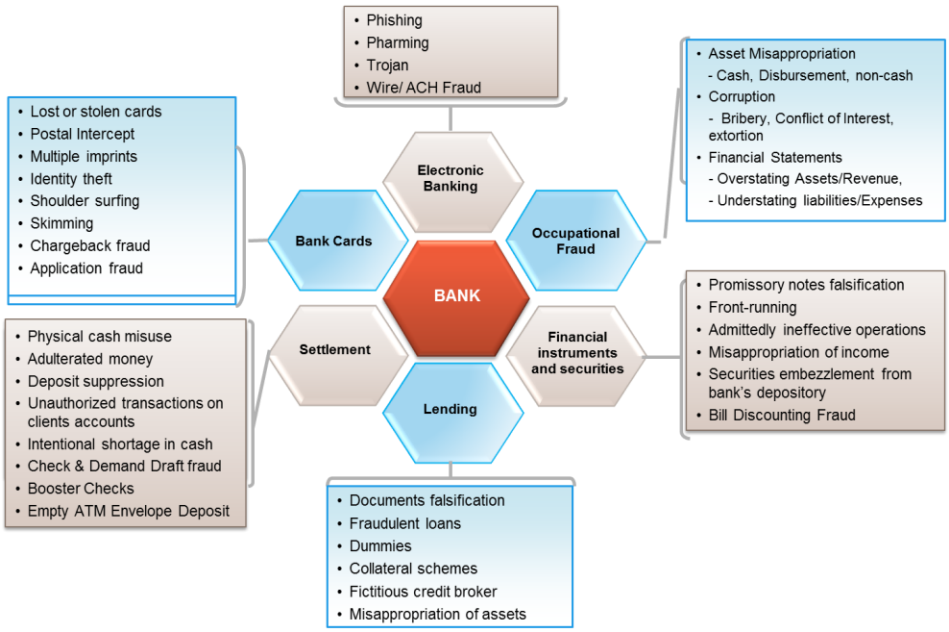
This paper looks at the common weaknesses to which banking customers using cards and online banking for executing transactions are exposed to. It focuses mainly on skimming and online frauds, probes the nature of these frauds and reveals the newer trends within these fraud types.

Further, this paper explains how banks have been trying to control these frauds by improving their systems and processes. It is evident that it requires considerable investment in systems /processes to improve the fraud monitoring and detecting capabilities. Small and medium banks, with limited IT budgets or fund constraints, have not been able to keep pace with the newer techniques developed by fraudsters. Their ability to adopt newer /better technology for prevention, detection & early warning of fraud being low , they are losing millions of dollars in addition to customer confidence.

We've made an effort to suggest how smaller and medium banks could use the services of IT Solutions providers, who have expertise in fraud prevention domain, in developing customized solutions for such banks, which can help them reduce the instances of fraud and thereby improve customer confidence and their bottom lines.

Common Banking Frauds

A bank is typically exposed to different types of frauds. The following diagram portrays the different frauds to which a bank is exposed.



In this article, we are limiting ourselves to Online (using Phishing) and Skimming frauds, which are the most common frauds.

Recent Trends

Being innovative is the business mantra for banks these day; We see innovation in terms of launching new products and services, providing additional features within already existing products and services or repositioning/ repacking existing products and services. Many a times, it so happens that in the scurry to beat the competition, new products or features are introduced without understanding the security implications.

Recent trends connote that fraudsters target victims through newer and unrelated channels like bank/ credit card related e-mails, merchant emails, social networking sites/ emails. The intent behind this is to catch the customers unaware.

In US, the trend has been to target Regional/ Community Banks than the Nationwide Banks. Global or Nationwide Banks have better resources to control frauds and launch campaigns to create awareness among their customers.

Newer forms of Phishing

Phishing continues to be a major problem for the retail banking industry. Phishing involves collecting information like usernames, passwords, credit card & debit card information from unsuspecting customers through electronic communication by impersonating oneself. The stolen information is then used by the fraudster to access the accounts of banking customers using online banking, mobile banking or telebanking channels and use the accounts for fraudulent purposes.

Newer forms of Phishing including Vishing and SMShing are gaining in popularity. Messages are sent to unsuspecting customers of the bank asking them to dial a phone number regarding problems with their bank account. Once the phone number (owned by the phisher, and provided by a Voice over IP service) is dialed, prompts ask customers to enter their account numbers and PIN. Instead of an email directing the bank's customer to a website, if the phisher sends an SMS or text message to the user's mobile phone asking him to click on a link, such a form of Phishing is called SMShing or Smishing or SMS Phishing.

Android mobile users are also easy targets to Phishing because of the presence of vulnerability in Android that allows for apps in the Android Market to steal user data. In fact, in the Android Software Development Kit (SDK), it is possible to push an application in the foreground, while another is being used. Using this, it is possible to display a fake bank login page to the user, while he/she is using the bank's legitimate app.

Mobile devices, when used for mbanking purposes can be dicey to its user as it security mechanism are not adequate and can be breached. Moreover, ease of download of software by the user in the marketplace which can malicious exists. Some of these software records key strokes and compromises sensitive personal information, usernames and passwords without the knowledge of the mobile user

Targeting the smaller banks

While the first phishing attempts were made indiscriminately in the expectation that some would be received by customers of a given bank or service, recent research has shown that phishers may in principle be able to determine which banks potential victims use, and target bogus e-mails accordingly.

Newer and unrelated channels

Fraudster are increasing trying to explore newer and unrelated channels like Bank/Credit Card statement emails, merchant emails, social networking sites/emails. The idea is to catch the customers unaware by using newer channels.

Using 'Man in the middle' attacks on mobile, fraudsters target mobile phones connected to a Wi-Fi network and redirect transactions through their own computers, allowing the fraudster to capture usernames and passwords.

How are Banks coping up?

Fraud management involves taking a holistic approach, blending tactical solutions with best practices /process in fraud strategy & operations. Fraud monitoring and detection one has to be clever and out-smart the fraudster. Hence Banks have to use advanced technology and make the life of fraudsters difficult. It's a continuous improvement cycle.

Not many banks have the systems to detect a fraud as it happens and block/prevent as it as it happens. However, a few banks have been in the fore in developing such systems. These

banks have invested heavily into systems which help them in:

- ✓ Detecting a live skimming fraud as it happens
- ✓ Knowing where and when the card was compromised (Common point of Compromise)
- ✓ Preventing the skimming fraud by blocking the compromised ATM or POS and hot listing the cards
- ✓ Refunding the clients who have been defrauded even before the client could detect the transaction
- ✓ Informing the client about the fraud and educating him/her on how to prevent such frauds in the future

Banks need to come out with robust models based on the different variables like customer usage patterns in terms of time-of-day and day-of-week profiles, percentage of spending in each merchant group category and transaction amount. These models are used in detecting live frauds. However, the models should not throw up legitimate transactions as suspected frauds. This may lead to blocking of customer cards and is an irritant for customers.

Banks need to introduce an additional layer of authentication in order to prevent card and online frauds. As of now, the first layer of authentication validates the account. The additional layer of authentication should be able to validate the identity of the person doing the transaction. For example, it could ask the person for his Date of birth, SSN, mobile number registered etc. which are only known to the individual and not stored on the card.

Before a transaction is executed, say a credit card payment or an online fund transfer, it should be assessed for fraud risk. The fraud risk score can be computed based on this transaction and the history & pattern of transactions made on the account which include day/time patterns, typical transaction amounts, common merchants / destination accounts, IMEI number or POS/ATM terminal ID or MAC address and segment to which the customer belongs.

How IT Providers can help Smaller Banks

The cost of fraud to a bank includes the direct loss due to the fraud, the cost of prevention and detection of fraud, cost of lost business (when replacing card or password) and deterrent effect on spread of the alternate channels of banking. Some of these costs can be measured directly while some are notional and cannot be precisely measured. Nevertheless, the cost of fraud has been going up steadily over the years.

In order to protect their customers, it is crucial for banks to consider real-time detection methods which can prevent losses from being sustained on customers' compromised cards. These tools allow institutions to monitor and immediately recognize suspicious transaction patterns, allowing them to act as soon as the fraudster makes an attempt and thereby prevent any losses.

Banks need to invest in fraud detection systems and early warning systems. This calls for more advanced analytics in card and online fraud detection. Also analytics should be capable of linking patterns in transactions across multiple channels. Given the vulnerabilities of transacting using mobiles, advanced analytics that monitor mobile device usage are required to detect fraud.

A good fraud detecting system classifies fraudulent transactions as fraudulent and legitimate transactions as legitimate.

Banks may also invest in automated case management systems which will assist them in investigation and resolving individual fraud cases. An automated case management system provides a framework to better manage and automate activities and processes for card and online frauds. Related cases can be linked and investigated together, investigative reports and evidence can be stored along with the cases, alerts can be set up at different milestones in the lifecycle of the case or based on SLAs.

Smaller & medium banks, most of which are regional banks, have smaller IT budgets. While the larger banks can go for state-of-the-art anti-fraud systems, the mid and small size banks can leverage the expertise of IT providers to build customized anti-fraud solutions to avoid the high costs of COTS.

Conclusion

Frauds are an inseparable part of any business. And so Banks too will have to deal with frauds no matter what level of security and scrutiny they build in. This is further complicated by the fact that fraudsters keep devising newer techniques of executing financial frauds.

This requires banks to invest in state-of-the-art IT systems to monitor, detect, block, investigate, analyze and prevent fraudulent transactions. Complicated models need to be developed which are capable of identifying fraud transactions by assigning it a fraud risk score.

Further these models need to be updated frequently and newer models should be added keeping in pace with the newer techniques developed by fraudsters. As soon as the fraud risk score exceeds a particular threshold, the transaction needs to be blocked before it is executed. The system has a time window of a few milliseconds to respond and block a transaction; else the transaction is executed as a normal transaction.

Next the system needs to identity the point of compromise, which is very important is preventing further frauds being committed on other customer accounts. A case management system is required to keep an ordered record of different fraud instances, the investigations into the frauds and reimbursement to clients where required.

Implementing the best of breed process and sophisticated systems requires constant investment in IT systems and processes. While the big banks, with huge IT budgets can afford to invest heavily in anti-fraud systems, the regional banks, with limited IT budgets, are not able to do so. Hence, they are increasingly being targeted by fraudsters.

On the other hand, there are many IT providers who have gained sufficient expertise in developing customized anti-fraud systems for their customers. Small and medium banks could leverage such an experience to implement customized systems to take care of their anti-fraud requirements. This will save them from the high costs of COTS Y-o-Y as well as improve their bottom line by achieving saving in fraud related costs.

Domain Competency Group
Financial Services

Collabera Solution

RMZ Ecospace, 4A Block, 5th Floor, Bellandur Village, Outer Ring Road, Marathahalli, Bangalore, Karnataka - 560 037 India

Phone: +91 80 4071 1999

Fax: +91 80 4161 3705

REFERENCES:

- www.fico.com
- www.aciworldwide.com
- www.forrester.com
- www.tapn.com
- www.gartner.com