An Approach to Detect Fraud at Account Level

Pankaj Richhariya*1, Dr. Prashant Kumar Singh*2
*1PhD Scholar, CSE, Dr. K.N. Modi University, Newai India

Abstract—With the arrival of new technologies for the communications, payment cards transaction increasing rapidly day to day. Payment cards fraud such as Credit card/Debit card fraud is a critical and rising problem which become progressively widespread in recent years. There is a necessity of an operative system that detects frauds very effectively at account level. Hence it turn out to be necessary that the users require to stay a step forward in this situation. Banks have experienced an growth in deposits in the wake of the stock market fall of 2008, as money fled the market in search of secure place and protections from the further losses. This signaled a return by the banking industry to one of its core principles. Deposit growth and preservation is critical for bring back stability in the banking system, and banks are progressing their efforts on this vital funding activity. However an risen in deposits raises the threat of another, uninvited increase- specifically, in deposit account fraud.

Keywords— Fraud detection, customer level fraud, account profile, account fraud, channel specific

I. INTRODUCTION

Banks historically sought to combat fraud involving demand deposit accounts (DDAs) with channel monitoring strategies. With the proliferation of account access points, however, channel monitoring is running up against serious limitations. Banks must implement cross channel fraud prevention capabilities as 35% of deposit account fraud losses at regional and super regional US banks stem from cross-channel fraud.

Econometric tool, composed with the techniques, is mainly working within the credit scoring process to assist organizations determine whether to issue credit to customers who apply for it [1][2][3][4][5]. Channel monitoring play an important role in any fraud detection and risk management strategy includes multiple channels building it critical to monitor at the customer and account level for behavioural indicators of threat or possible fraud.

Monitoring in Account level is turn out to be a requirement in the attempt to prevent fraud losses. A novel creation of detection tools will allow banks to connect applications of decision-making across multiple channels, providing a more robust scene of customer behaviour. This paper studies:

- Now a day in deposit accounts where the business is to fight against fraud and to discover risk.
- Seeing the multiple channel/exit points and various banking behaviors how the fraud is detected in the deposit account.
- Why it’s critical that deposit organizations use personalized, adaptive profiling to observe the behavior of customer and account.
- The influence of related decisions in observing customer behavior across multiple channels.

II. TODAY’S SCENARIO

For a particular channels now a day organizations uses various tools and technologies of risk assessment and fraud. Though some of them address the rising problem of organization or fraud of multi-channel. Policies of deposit account fraud are normally planned operationally around particular alerting systems as shown in figure 1. Furthermore, operational budgets and losses are aligned by channel. With the increasing trend of cross-channel fraud, financial organizations are seeking for approaches to improve fraud detection and management at the deposit account level. For examples, debit card operations are trending toward alignment with retail banking, as opposed to the past when they were grouped under “card” detection and operations.

One method that organizations are leveraging to assist in cross-channel operations and fraud management is enterprise case management. Work process consolidation is a noteworthy and positive trend because it allows for cross-training and the ability to pass cases between disparate operations centers. Traditionally, a bank’s channel-specific operation and
investigation centers utilized several different systems, user interfaces and investigative workflows—although in some cases, targeting the same account. Aggregating multiple case alerts into one account view eliminates bottlenecks, simplifies access and streamlines case movement through the system. Alert consolidators, however, are not the panacea to enterprise or multi-channel frauds. They are still channel-specific and the fraud strategies are not connected in a way to identify account-level and customer-level frauds. They do not, therefore, reduce false-negative rates.

There is also increased complexity in an alert consolidator. Analyst must drill down into each alert to get views into what might be going on. And there’s the risk that case effectiveness is often driven by the weakest alerting system, which typically has the greatest false-positive rate. In any case of the current methods used, organizations still face developing fraud and risk because of the extreme nature of the deposit account:

- In the banking system there are many access and exit points.
- The technologies have been introduced in the banks decrease the fraud in moving money in and out of accounts or from one account to other.
- The behavior of the customers are changeable and varied.
- The fraudsters are come to be further planned and complex.
- Controls tend to be one-dimensional with the threshold-based rules.

To effect the ability to manage risk and fraud effectively there are three additional issues challenges the current deposit organizations.

1. **Deposit it account fraud management has the opportunity to standardize fraud classifications and measurements, as is the case with card fraud.** The lack of standardized fraud classifications is evident throughout the industry. Most banks describe their fraud problem as schemes that are focused on specific channels. In many cases, fraud in different channels is related and exhibits significant overlap. The variance is definition is probably based on how each bank is measuring its problem, or whether it is focused on the point of entry or area of loss.

2. **Banks are often playing catch-up with evolving multi-channel frauds.** Once geared primarily to identify check fraud, banks must now scrutinize volumes of data and scenarios that reflect the faster and more anonymous nature of multiple access channels to funds. It is common to find deposit account fraud prevention and detection operations organized according to specific channels with specific fraud strategies. Access to each “silo” can require journeying through different information management systems, each with unique data, rules and work flows. By not capturing all the critical data on a customer in one easily accessed central location, banks lose time in constructing cases and miss seeing the big picture. Efficiency suffers and informed decision-making is compromised. Computing that issue is the integrity of the information itself; is it reliable? Moreover, in many cases, when the organizations information management systems are constructed, fraud and risk programs were not a component on the data structure.

3. **Lack of centralized fraud detection and prevention strategies in several financial organizations.** Vital fraud and risk policies and strategies are often executed or over-ridden at the branch or regional office. The legacy of branch-only banking has shaped a culture in which tellers and branch managers may provide full funds availability on a suspicious deposit (possibly to avoid conflict with a customer) even though it is often the head office that “owns” fraud and risk losses.

**III. COSTS AND SIGNIFICANCES**

Many banks lack effective tools and technologies to detect fraud and assess risk in the deposits arena, and the consequences are well documented.

In the survey of 2009 survey American Bankers Association studied the foremost risks against deposit accounts, recent and expected check fraud losses, and other fraud correlated topics both by complete business trends and by bank asset size. It is found that:

- Survey members recognized customer persecution scams, fraudulent check deposit and signature debit card fraud as the topmost three risks opposed to banks deposit accounts in the next 12 months.
- Among check fraud losses, 26% are associated with new accounts.
- Payment fraud increased in remote channels from 2006-2008 (not-on-us
ATM 14%, on-us ATM 7%, wire 15%) while deposit fraud continues its prevalence via the branch (81%).

- Banks reported an increase in social engineering fraud targeting the call centers.
- ACH fraud incidents rose dramatically-up 537% since 2006.
- Between 2006-2008, the reported incidence of check fraud increased by 35% but the gross loss per case decreased by 22%, resulting in slightly higher gross loss (slightly above $1bn).

The problem is international. Despite the proliferation of multi-factor authentication controls, online fraud has increased 132% from 2007 to 2008 within the UK, according to APACS, the UK’s top payment industry association.

Meanwhile, the growth in online banking and commerce, while reducing costs for institutions and improving convenience for consumers, has also created a fertile arena for fraud, despite the widespread industry adoption of security controls requiring two- and three-factor authentication. According to the internet crime complaint center’s 2008 report, online fraud losses quadrupled, from $68 to 265 million, between 2004 and 2008.

IV. CHALLENGE OF BALANCE

Perhaps more than any other industry, banks must strike a fine balance between taking measures to prevent fraud which is, of course, in their customer’s best interest and keeping positive relations with their good customers. In detecting fraud and prevention loss in credited accounts and linked accounts, there are various concerns that finally build and assistance a banks brand status inside its market. These contain:

- Accessing the accounts securely
- Monitoring compliance
- Recognition of unauthorized access
- Balance of centralized and decentralized fraud control.
- Optimization of funds availability for improved customer satisfaction
- Liquidity (crucial in today’s economic climate)
- Optimization of free revenue while prevention overdraft fraud and credit losses
- Multi-channel access to funds
- Variety of banking associations across customer base

Particularly the role of bank’s role, with deposit accounts, is to be a caretaker of its customer funds and to reduce friction points for funds running into, out of and amongst accounts. Though, anyplace there’s money, there’s bound to be threatening determined. Unluckily, by reason of the complexity of multi-access points into an account, there are various combinations of approaches for fraudsters to ready the deposit system, permitting fraud losses to slip within undetected.

V. A NOVEL OUTLOOK

Given this environment, and recognizing that currently fraud schemes are very complex observing and managing fraud and risk valuation needs a novel outlook the perfect view from the account level. This convenience point is more beneficial than detection and work handles around specific channels, and particular fraud schemes within channels, because it takes into consideration the behaviour of the accountholder.

By behaviour we mean how the customer interacts with the account, including both monetary activity and non-monetary activity such as altering personal information or password. Understanding this interaction is the key to detecting anomalous behaviour on the account, which may indicate account takeover or that the authorized accountholder has malicious intent. Deposit behaviour is also frequent indicator of potential first-party fraud and abuse on related accounts, such as linked credit lines.

Unusual behaviour also might be indicative of credit risk rather than intentionally fraud. From a strategic point of view, fraud and risk behaviours and the resulting account action pose the challenge of striking a balance among loss mitigation, customer satisfaction and revenue optimization. As a result, there is a growing trend in the banking industry to incorporate fraud and credit risk strategies together in loss prevention strategies. Deposit organizations have a chance to associate risk assessment and fraud detection via real-time decisions, directing to proactive investigation and action.

VI. EMPLOYING ACCOUNT-LEVEL BEHAVIOUR TO DETECT MULTI-DIMENSIONAL FRAUD

The first step to recognizing abnormal accountholder behaviour is certifying that controls are computing and recognizing the behaviour trends of the cardholder.

- Has this person currently shown a risen or reduction in deposit?
- Has the rate of their payments raised or reduced?
- Has their payee/payer distribution shifted?
- Have their payment access methods and amounts shifted recently?
- Have they recently interfaced with the customer service department to make changes to their account (change of address or phone, change of PIN etc.)?

Without the ability to encapsulate account holder behaviour, it is not possible to detect fraud on the portfolio thoroughly and quickly. Most of today’s fraud detection systems make use of conditional rules
or segmentation. These threshold policies do not take into consideration other crucial factors such as the trends, velocity and timing of the customer’s actions-customer behaviour over time, both recent and longer-term historical patterns. These policies are the reason that deposit institutions need to use individualized adaptive profiling to monitor account holder behaviour and events.

VII. THE POTENTIAL OF RELATED DECISIONS

By merging risk assessment and fraud detection, a bank has the capability to find fraud and reduce losses, building up the satisfaction of the customer and increase fee revenue opportunities. We offers a sophisticated combination of rules based technology, artificial intelligence analytics case management and workflow, enabling extensive, cost-effective fraud detection. And approach to fraud in deposit account is to use monetary transactions and non-monetary events to update the account-level and customer-level profiles to produce a fraud score. Figure 2 shows a number of accounts belonging to a customer; they might be a single account, joint account and business account. We produces an account and customer score. The score of account make available a probability that the account is behaving abnormal. And the score of customer provides a probability of the customers risk to the bank.

The score on the accounts can be differ from one another at any point and from overall score of the customers. Therefore the irregular use on the account of a customer’s business account can score high, signifying account takeover or suspicious activity. The customer score here is low at 240, showing that the customer is a fraudster.

These scores, along with additional data, become an input into FICO TRAID customer manager, FICO account and customer level decision management solution.

For example, TRAID customer manager can use the Falcon scores to make real time decisions on funds availability. If the Falcon account score is high with indications that there is account takeover, TRAID customer manager can decrease or stop funds availability on specified channels that are not normally utilized by the account holder, thus thwarting unauthorized access. TRAID customer manager may also use a low customer score to assume more risk on a higher risk funds availability transaction with a valued customer.

The influence of placing analytics into an actionable decision offers the bank with several benefits:

- The satisfaction of the customer is improved and there is a better bank customer relationship by providing a personalized banking experience.
- Observing proactive account with the combination of transaction behavior into account level management prior to cycle cuts.
- Initial identification and instant action of fraud that otherwise would be concealed in the collections workflow.
- Timely identification and proactive action of accounts displaying credit risk.
- The capability to apply policy compliance and changes across the lifecycle. In some cases, the ability to power existing infrastructure, reducing capital investments.

TRAID based decisions can be triggered either by real-time events or by a real-time/near-time event that results in a high fraud score on an account and/or customer.

Falcon Fraud Manager 6 and TRAID customer are part of the FICO Decision Management Suite, a set of applications sharing a common architecture that allows financial institutions to automate, improve and connect decisions across the customer lifecycle. This enables the fraud detection system and customer management system to communicate with one another in a seamless solution.

Step by Step Process

Improving deposit account fraud and risk management is a journey, not a destination. It’s a long term investment in detecting cross-channel frauds. Thus, we advocate a step-by-step approach to achieving “complete coverage” by first implementing controls on deposits and withdrawals via ATM and all items. Account-level detection and treatment can happen immediately with those two feeds(in conjunction, of course, with customer master file updates). The value of ACH/EFT or online banking/bill-pay is up to the bank to decide. Each phase of the implementation should be funded by the return on investment from the preceding phase.

VIII. CONCLUSION

Deposits are this period’s leading source of bank income and a rising target for fraudsters globally. Predictive analytics and detection in real time are an
exclusive means of resisting the attack and assessing risk. The author introduces advanced analytics and the capability to do multi-product, multi-product case management and detection along with power the existing set-up for associated decisions. The results empower a bank to determine more fraud, develop well customer relationships and provide larger fee revenue opportunities.

ACKNOWLEDGMENT
The authors wish to thank Prof Suresh, Bhopal Institute of Technology & Science and Dr. Arvind Kourav, Globus Engineering College, Bhopal for proper guidance

REFERENCES