GLOBAL SIX SIGMA AWARD SUBMISSION

Best Project Achievement in Business Enabling Processes – HR / IT / Regulatory / Risk Management

Canadian Imperial Bank of Commerce (CIBC) is a leading North American financial institution with annual revenues of over $3.7 billion. CIBC Retail Markets provides a full range of products and services to almost 11 million personal, business and wealth management clients served through 1,058 retail branches, over 3,780 ABMs and 24/7 through online and telephone banking services.

Through application of the Lean Six Sigma (LSS) methodology to its Debit Card Fraud Prevention processes over a 6 month period, CIBC achieved the following major improvements:

- End-to-end lead time from alert to completion reduced by over **80%**
- Average losses per incident reduced by more than **45%**
- Implemented changes to reduce debit card fraud losses by more than **$7 million***
- Identified other opportunities for additional savings estimated at **$10 million*** as result of proposed technology enhancements

* Based on a 5 year NPV (15.5% pre-tax discount rate)

The strategic objectives of the project

Debit card fraud is a reality that all retail banks are faced with in today's marketplace. Historically, loss trends due to debit card fraud were increasing year over year culminating in an F2007 increase of 30%. As fraud techniques and fraudsters' behaviours have evolved and become more sophisticated, CIBC has been faced with an increased number of fraud instances and an increased level of complexity in the fraud prevention process. The mitigation of reputation, financial, and client risks were seen as the major strategic objective for the debit card fraud project.

The amplified fraud activity had increased the workload activity within the time sensitive/critical role of the Common Points of Purchase (CPP) team. As a result, the National Risk Monitoring (NRM) team engaged the Process Engineering group to investigate the current Common Points of Purchase process and identify key root causes and solutions for mitigating financial and reputational risk relating to debit card fraud.

The CPP process consists of four major steps:

1. A suspect transaction is identified by other teams monitoring the debit cards and that particular transaction is referred to the CPP team.
2. As there are multiple identification sources, the referrals are queued for investigation to determine if the suspect transaction is fraudulent or not. Confirmed fraud on multiple cards at the same transaction location are required to identify a compromised Common Point of Purchase (CPP).
3. Once a compromised CPP is identified, the suspect cards are extracted and blocked to prevent further fraud from occurring.
4. Every card is then messaged and the card holder is informed of his or her card being blocked and new cards/ passwords are activated.

In August 2008, a project was initiated, a project team was formed (including 1 Black Belt, 2 Green Belts and 2 Process Experts) and project governance was established with sponsorship at executive level from Integrated Business Control Services within Retail Markets. A cross-functional team was formed with members from the core Retail Markets Process Engineering group, in partnership with business subject matter experts from NRM. The team followed a lean Six Sigma (LSS) methodology adopted by CIBC in 2002.

Assessing the current state, the project team identified that lengthy queue and process times involving numerous applications and multiple sources of non-prioritized referrals (suspect transactions that require further investigation) can delay the assessment of the next referral, causing also a delay in finding other CPPs. This, in turn leaves fraudsters with a larger timeframe and opportunity to defraud more compromised cards, and has caused NRM's average loss per card to increase (average 15% in F2007).

The goal of the project was to leverage LSS methodology to evaluate current state, identify root causes, design and implement non-technology improvements of CPP process and identify technology-related improvements that will help reduce the debit card fraud losses. Specific goals were established to reduce the process end-to-end cycle time, reduce loss amount per incident, and quantify potential benefits as result of implementing technology automation.

In order to reduce the financial risk exposure while quickly improving the client and employee experience, the project focused initially on improving existing CPP process without any technology change. This allowed benefits to be realized through the process reengineering by identifying and removing waste, as well as removing non-time sensitive activities

from critical path to newly assigned administration employees. In essence, this generated an increase in capacity for the front-end analysts, which allowed them to investigate and address more alerts in the same period of time without expanding the number of analysts.

The second phase of the project was focused on identifying long-term solutions that required modifications of existing technology to automate steps in the process and improve the information flow required to make real-time decisions in investigating debit card fraud. Ultimately, this will result in further loss reductions and increased client and employee satisfaction.

As a sign of commitment from senior executives and to provide necessary guidance and approvals, a Steering Committee was formed and resources were prioritized for this project. The core working team of LSS practitioners met with the Steering Committee on a monthly basis throughout the life of the project.

By committing to improve a process that will reduce debit card fraud, and delivering against the commitment, the project goal and deliverables fully supported CIBC priorities to strengthen the risk management, improve productivity and enhance client experience.

Project implementation and timeline

In August of 2008, an operational review of the process was initiated by National Risk Monitoring. By September, the project scope was expanded to include the long-term technology recommendations and a finalized project governance model. Under the LSS methodology, a Define, Measure, Analyze, Improve, Control (DMAIC) approach was adopted. Stakeholders were identified from impacted Lines of Business and employees from NRM teams who are actually engaged in the daily process.

From August to October of 2008, the project team focused on collecting Voice of Customer (VOC) and processing data to determine Critical to Quality (CTQ) components of the process. Through extensive data collection and analysis, process capability was assessed and baseline performance measurements set. Current state Value Stream Maps (VSMs) starting at the initial suspect transaction were developed and validated with those employees who use the processes on a daily basis.

In the next months, with the help of collaborative brainstorming sessions with subject matter experts from all areas of the process, root causes (leveraging Fishbone) were determined and potential solutions identified. A prioritization matrix was used to help assess the options and ensure Critical To Quality (CTQ) measures were addressed. Future State design maps were created and reviewed and recommendations for process improvements were finalized by the end of October.

In November 2008, the team gained approvals from the executive sponsors to move forward with implementing the non-technology related recommendations. Through ongoing consultation with stakeholders, and rigorous risk-proofing (ie. FMEA) and change management tools, design changes were finalized to include improvements in:

Front End Analyst Activities

- Replaced batch and queue processing with continuous flow
- Introduced checklists by role as part of standard operating procedures
- Developed visual controls to assess the progress of each investigation
- Eliminated non time sensitive activities to allow more time for investigation
- Introduced production huddles and visual management tools such as a process dashboards
- Developed a workforce allocation and forecasting tool for improved resource planning

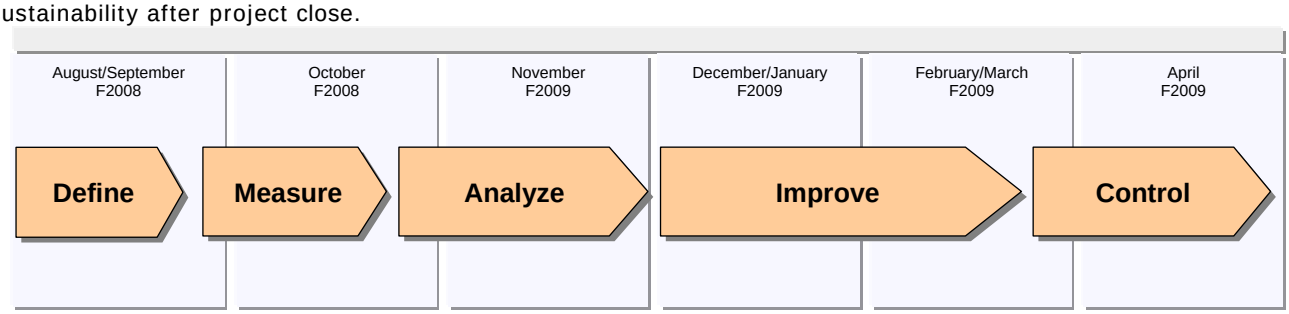
Administrative Function

- Introduced a new administrative position to execute non-core activities
- Developed a tracking tool to monitor all investigations to improve detection of patterns
- Executed cycle time reduction by performing activities in parallel that are not on critical path
- Implemented regular and automated reporting of performance measurement metrics
- Developed cross training for Analyst back-up, when required, due to volume increases or staffing issues

The first wave of changes was piloted in December 2008 as an increase in debit card fraud was reported in the marketplace. Procedures and checklists were developed and reviewed with stakeholders to include all changes and enhancements applied in the pilot. By February 2009 all changes were implemented and procedures were finalized.

As per the CIBC LSS methodology, a 3 month control phase was conducted by the team from February to April 2009. During this time, detailed process metrics were collected, analyzed, and distributed weekly to key stakeholders via a

process dashboard. The objective of this phase is to ensure realization of benefits, address issues, and ensure sustainability after project close.



The size of project challenge

Interac Association is responsible for the network that allows Canadians to access their money through bank machines and retail point of sale terminals. According to its numbers (*www.interac.ca*), out of the 3.7 billion transactions occurring in 2008, 148,000 debit card victims were reimbursed a total of $104.5 million due to debit card fraud. This represents roughly a 70% increase in funds reimbursed over 2004 when $60 million was defrauded from 49,000 victims.

Skimming is the loss of funds through stolen debit card information. Fraudsters typically compromise ABM machines or point-of-sale (POS) devices (used in stores and restaurants) to acquire multiple debit card numbers and associated pin codes. Counterfeit cards are created using this stolen information and then used to withdraw funds from the compromised accounts. Fraudsters are typically part of organized criminal groups who have the resources to withdraw thousands of dollars using hundreds of counterfeit debit cards within minutes.

CIBC's National Risk Monitoring group investigated over 25,000 high risk debit card transactions. An additional 9,500 CPPs identified by other Financial Institutions were addressed, as part of partnership program involving the major financial institutions to combat debit card fraud.

There are 12 different sources that feed suspected fraudulent transactions into the CPP team and each source needs to be prioritized and staffed. There is a significant amount of variation in the investigation time as it is dependent on the number of ABM and POS devices that need to be checked for a particular suspected transaction. The variation in investigation time makes resourcing and prioritizing of sources very challenging.

Adding to the complexity, the type of CPP (ABM or POS) and the number of cards compromised for a particular CPP impacts the investigation time. ABM and POS tampers have different fraud spend patterns and at the start of the investigation step the type of the CPP is unknown. Generally, ABM tampers are more difficult to identify because there are fewer cards compromised. Additionally, the flow of information and staffing structure was not set-up to properly facilitate investigation, especially for ABM tampers.

The CPP process involves 12 different applications and requires a minimum of 80 screens per CPP. In addition to working with a complicated process, the CPP team has to complete their investigations and block cards within a very narrow timeframe to prevent losses, especially during a live skim. Each minute of a live skim costs approximately $150 per compromised card.

The NRM skim loss average has increased over 30% in 2008 with average spot (monthly) losses increasing close to 60%. This heightened fraud activity has increased the workload within the time sensitive/critical role of the Common Points of Purchase (CPP) team.

The organizational impact of the NRM CPP project

The impact of the project was considerable. Debit card fraud is a growing and major concern not only for CIBC, but for all Canadian financial institutions. The end result of being able to detect the fraud faster and action the affected cards more efficiently is two fold: significantly decreased losses overall; and a strong, proactive client service experience that underscores the message that CIBC is taking active steps in preventing criminal activities to affect our clients.

At the end of phase one of the project, annualized loss avoidance was $2 million. In addition, long term solutions recommended by the project provided opportunities to justify an investment in technology of more than $6 million with a payback period of less than 3 years. The figures will likely be even higher as they consider the current static volumes, as opposed to forecasts which indicate an overall increase in debit card fraud activity in the future.

The lead time to investigate an alert decreased by 83%. This was accomplished by eliminating non-value add activities from the critical path and redistributing the work to an administrative function, which increased the front end analysts capacity by 28%.

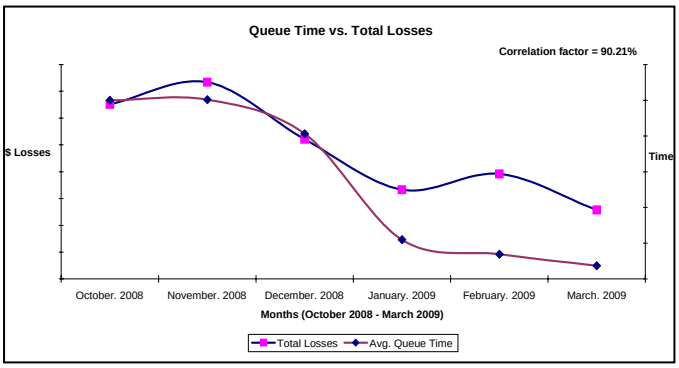
Average ABM loss per incident decreased by 46%. This was accomplished by being able to identify the defrauded cards faster and action (block and message the cards) before fraudsters could use them.

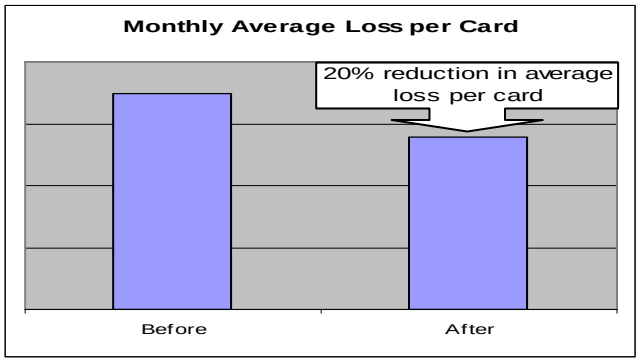
Monthly average loss per debit card decreased by more than 20%. This was accomplished by being able to block the cards faster, so they can not be used again for fraud.

All of this resulted in an increase in client satisfaction. By automating the messaging, clients are proactively informed of the fraud even before noticing it themselves, and no replacement card is required anymore. This is in addition to the figures mentioned above and has not been quantified by this project.

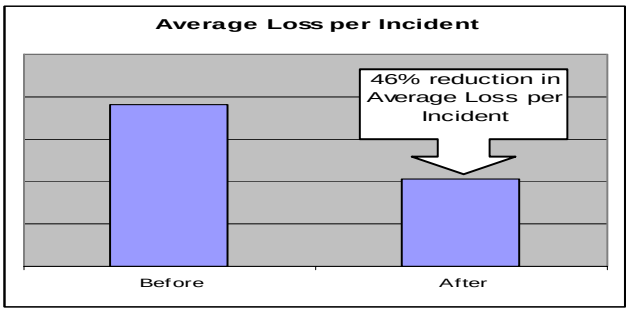
A key component of the CIBC LSS methodology is ensuring benefits realized are sustainable and that there is ongoing process visibility and accountability. A process dashboard was implemented to monitor and create visibility on process performance. The dashboard is a collection of key metrics collected automatically from underlying systems and distributed to a group of stakeholders identified as having an ongoing role in ensuring process performance remains in control.

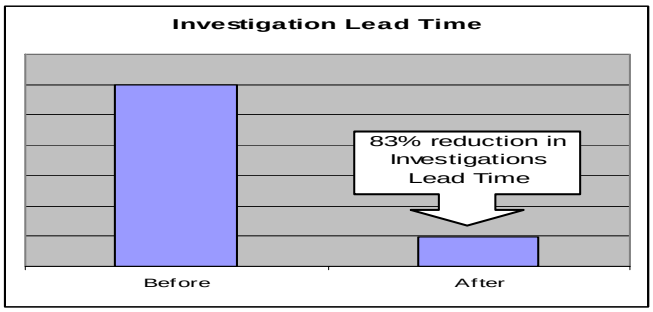
The business results of the NRM CPP project





A strong correlation was identified between debit card losses and the investigation lead time. Run charts indicate similar trends.
The amount of losses per card decreased by 20%, which indicates that fewer cards are used multiple times for fraud before being addressed.





As the result of process improvements, the average loss encountered per incident decreased by 46%. This is an indication of cards being found and addressed faster; therefore fewer cards are involved in one incident.
A reduction of investigation lead-time by 83% contributed strongly to an overall loss avoidance of more than $2 million (annualized).