Deloitte.

Tipping the triangle

Predictive analytics to mitigate empty envelope fraud

Content

Identifying fraudsters in a crowd 1

Understanding the impact of fraud 3

Current challenges in financial fraud 4

Balancing customer experience and corporate security 4

Customer and operational costs of rule-based detection 4

Improving fraud risk diagnostics 5

Analytics for prevention, detection, and mitigation 5

Scientific solutions for financial security 6

Account applicant risk scoring 6

Behavioural risk monitoring 7

Intelligent fraud management systems 8

Account applicant risk scoring 9

Behavioural risk monitoring 10

Making a difference through advanced analytics 10

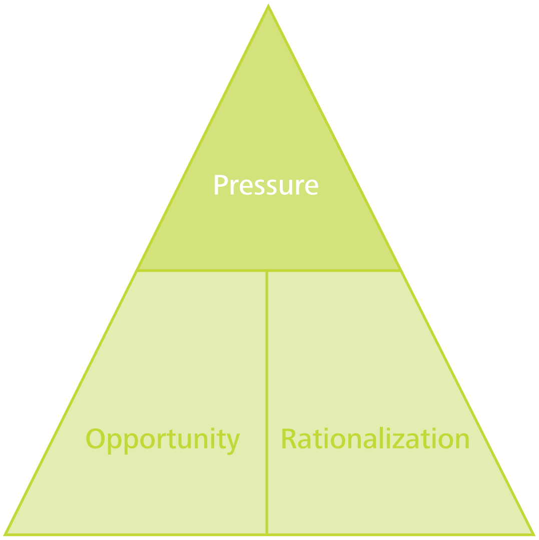
Endnotes & references 12

Identifying fraudsters in a crowd

Fraud is driven by an intentional human element that continuously mutates and evolves, making it a crime that is notoriously difficult to contain. As a result, detecting and mitigating the impacts of fraud remain ongoing concerns for the financial services industry.

Focusing on that human element, the Fraud Triangle (Figure 1) illustrates three key factors that enable individuals to commit fraud: pressure, opportunity and rationalization.[1] The economic stress of the past few years has seen motive (or pressure) and opportunity on the rise. Motive arises from the financial pressure individuals feel when they confront personal challenges such as debt, addiction or greed; opportunity defines the way in which a person might inappropriately resolve their financial pressures, given a low perceived risk of detection. The final tenet of the triangle is rationalization, which sees an individual self-justifying the fraud act as necessary in order to silence his conscience.

Figure 1 – Fraud triangle



Fraud (noun):

1. Intentional perversion of truth to induce another to part with something of value
2. An act of deceiving or misrepresenting (Merriam-Webster)

The goal is to develop solutions that incorporate these predictive techniques along with the continuous monitoring of data collected at large financial institutions.

The effects of this all-too-human equation when it culminates in financial fraud are felt by both industry and society. For example, organized crime has benefited significantly by developing highly complex and coordinated fraud methods, including identity theft, document falsification and collusion with insiders who help execute these schemes while attempting to evade detection. The speed and adaptability of attacks conducted by opportunistic individuals acting on their own, combined with the scope of those by organized crime, intensify the losses felt by financial institutions. At the same time, account takeovers and new account fraud affect people in the lowest income bracket at disproportionately high rates.[2]

However, as the volume of data grows and the industry focuses more closely on detection, analytics has evolved to provide proactive, real-time insights into fraud behaviours and activities. The goal is to develop solutions that incorporate these predictive techniques along with the continuous monitoring of data collected at large financial institutions. By applying analytics to financial data within a proactive framework, fraud can be prevented, detected and mitigated to better manage financial risk.

To demonstrate the value of this approach, Deloitte's advanced analytics team partnered with a large Canadian bank ('the Bank') to exchange ideas, resources and subject matter expertise. This paper, a collaborative product of that partnership, looks at the impacts of fraud, at challenges in the current fraud landscape and at the ways in which new analytics solutions are reducing risk and improving financial security.

Understanding fraud and its impacts

Fraud is both evolutionary in nature and evasive by design. Identifying it involves collecting enough financial information from across an organization to justify legal action. This, however, often poses a challenge. Although fraud is a significant source of cost, financial institutions struggle to accurately quantify its monetary impact on their bottom line:

- A recent survey estimated that the typical organization loses 5% of its revenues to fraud each year. Applied to the estimated 2011 gross world product, this figure translates to a potential projected global fraud loss of more than $3.5 trillion. This equates to roughly $500 per global citizen.[3]
- Statistics Canada in 2008 showed that $500M of bank-related fraud involved debit cards; $300M was associated with fraudulent cheques; and $100M was in worthless deposits.[4] Since 2008, the rate of empty envelope deposit fraud has increased relative to other types of bank-related fraud.[5]

Such fraudulent activity often involves complex interactions between multiple parties, and detecting it requires a discerning approach that can sense complex relationships and quickly highlight risky behaviour.

> Fraud is both evolutionary in nature and evasive by design. Identifying it involves collecting enough financial information from across an organization to justify legal action. This, however, often poses a challenge.

Current challenges in financial fraud

As statistics show, Canada is no stranger to fraudulent activity like empty envelope deposits, and recent legislative changes to consumer deposit laws have aggravated this threat. In August 2012, access to funds regulations came into effect requiring banks to make the first $100 of all funds deposited by cheque available immediately for withdrawal[6]. This law has activated the opportunity corner of the Fraud Triangle: during the latter half of 2012, the rate of empty envelope deposits received at branches and ATMs tripled. In addition to the core costs of misappropriated funds, banks feel ancillary consequences of such crimes at the operational and consumer level.

Beyond the risk of specific frauds, financial institutions face a variety of fraud-related challenges, including balancing customer experience and corporate security; the customer and operational costs of rule-based detection; and the need to improve fraud risk diagnostics.

Fraud-related challenge

Balancing customer experience and corporate security

Consider the following scenario: A married couple, new to the city, has recently moved into a 15-year old house and proceeds to their local bank branch to open a joint chequing account. After the couple has provided their personal information and agreed to a credit bureau review, the bank employee excuses herself from the conversation. She has just been notified that the family's new address has been previously compromised by fraudulent activity. The operational team must now complete additional due diligence to decide whether or not to restrict access to the bank's services.

This scenario highlights the challenge of balancing a positive customer experience with strong fraud management initiatives. Customers want their involvement with the bank to be seamless and pleasant while presuming the financial institution is actively engaged in fraud management. This balance requires thoughtful and delicate verification procedures that do not negatively impact the customer.

Customer and operational costs of rule-based detection

At large financial institutions, millions of customer transactions flow through a series of electronic monitoring systems daily. Transactions are compared against historical patterns and other customer information. Automated systems flag suspicious activity for follow-up by operational personnel who investigate identified accounts for potential risk of fraud.

The process of monitoring and flagging accounts casts a very wide net. Most clients honour their customer agreements and, when flagged, do not necessarily warrant further investigation. These alerts and subsequent follow-ups can inconvenience customers and generate additional work and costs. Fraudsters understand this and can exploit such investigative delays, exacerbating fraud losses.

Improving fraud risk diagnostics

Corporate security can be reinforced by augmenting existing systems for account applicant screening and transaction monitoring. New application screening methods focus on identifying individuals and/or addresses associated with prior violations of customer agreements. Once a new account is opened, monitoring systems apply rules to filter and flag suspicious transactional scenarios. While generally successful in detecting fraud, these methodologies can be enhanced to abate further financial loss and customer impact.

Account applicant risk scoring

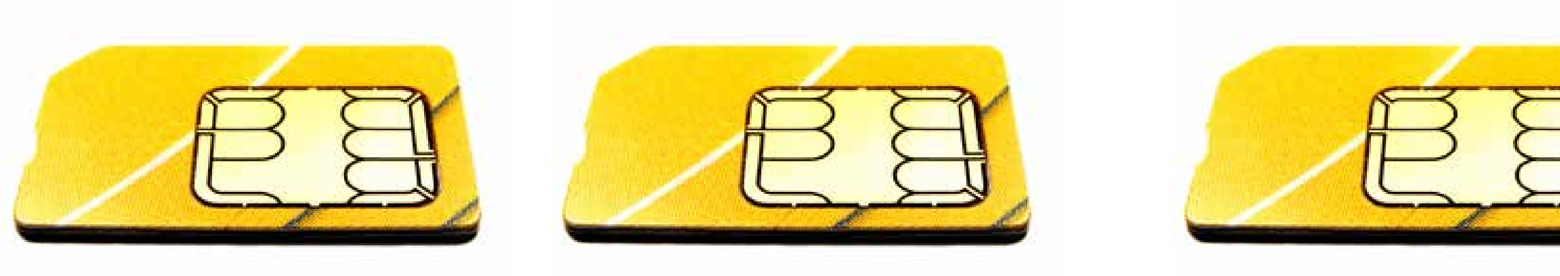
The married couple in our earlier scenario was flagged as high risk because their address matched one that had been previously compromised; however, considering other characteristics of their application profile could have simplified the process. Agreeing to a credit bureau check and applying for a joint account are two factors that significantly reduce the risk that the application was made with fraudulent intent. A holistic approach to profiling account applications can be used by operational staff to prioritize investigation.

Behavioural risk monitoring

Suspicious activity is presently identified using rules triggered against thresholds specified by human analysts. The rules are reactive in nature, in that they are defined by presupposed, potentially risky behavioural patterns (e.g., multiple aggressively timed withdrawals). Sleuthing by operational staff periodically results in new and updated patterns that must be encoded within a monitoring system; however, the overall process could be augmented by adopting a self-adaptive predictive modeling framework to identify and classify risky behaviours as soon as they arise.

Analytics for prevention, detection and mitigation

The volume and variety of Big Data that banks are currently collecting and warehousing has them well positioned to capitalize on advanced analytics. Hidden behavioural patterns that do not strictly adhere to known, a priori fraud topologies can be discovered in such data using synthesis, modeling and visualization. Incorporating analytic insights into existing application and transactional system design can directly address operational costs and relieve customer irritation.



Scientific solutions for financial security

Transactions are being executed at ever increasing speed and volume, and many financial institutions are moving toward a single, holistic client view where customer and transactional information no longer remain in silos separated by channel. New approaches to tracking fraudulent behaviour must therefore make effective use of state-of-the-art methods and algorithms that can tie together, analyze and interpret disjointed heterogeneous data sets from all channels.

Deloitte collaborated with the Bank to leverage their joint financial crime, advanced analytics and fraud management skills and experience to gain a deeper understanding of one particular type of fraud – empty envelope deposits. The resulting experience highlights the potential benefits of fraud mitigation tools that use advanced modeling techniques and can be deployed in environments that require security, privacy and cross-platform efficiency.

The joint team sought to understand fraudulent activity associated with the government's new consumer deposit legislation (mentioned earlier), which mandates the immediate available withdrawal of the first $100 of all funds deposited by cheque. The team focused on applying account applicant risk scoring and behavioural risk monitoring in the following ways:

Account applicant risk scoring: Build on the current new application process by scoring flagged applications according to risk level.

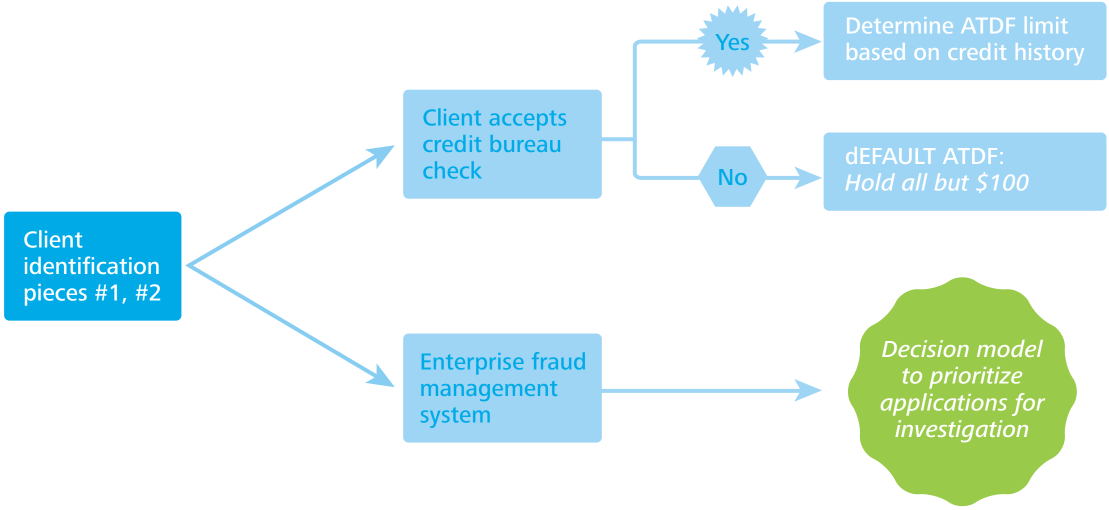
Behavioural risk monitoring: Leverage historical transactional data to interpret the behavioural profile of activity associated with empty envelope fraud.

Account applicant risk scoring

The account applicant risk scoring model helps operational staff prioritize flagged applications within the current onboarding process, as shown in the process excerpt in Figure 2. After customer application attributes are entered into enterprise fraud management software, the model computes a score based on the full set of application information. The score describes the propensity of a customer to exhibit non-compliance with regards to their service agreement and provides a guide to bank employees as they make decisions on prioritizing flagged applications for investigation.

Applying a risk-weighted score to the information captured on a customer application has already been proven useful in determining propensity for non-compliance. Deloitte applied this technique for a financial regulator, building a mathematical model to classify applicants by propensity to be non-compliant with exchange rules. This work enabled the regulator to prioritize existing compliance and investigative resources more efficiently. Financial institutions face similar challenges with respect to maximizing risk identification and optimizing limited security and investigative resources

Figure 2 – Prioritizing risky applications for review within the existing process


Client identification pieces #1, #2
Client accepts credit bureau check
Yes
Determine ATDF limit based on credit history
No
dEFAULT ATDF: *Hold all but $100*
Enterprise fraud management system
Decision model to prioritize applications for investigation

Behavioural risk monitoring

Identifying risky behavioural patterns begins with analyzing historical data to understand which activity profile is associated with empty envelope deposits. Isolating this activity reveals significant information.

Figure 3 shows the average elapsed time between successive withdrawals, deposits and balance checks initiated at ATMs. Behaviour differs markedly between regular accounts (those not exhibiting empty envelope deposits) and accounts where empty envelope deposit transactions have occurred.

Perpetrators begin by depositing an empty envelope and then withdrawing funds against the artificially increased balance. This happens relatively quickly; the average time between an empty envelope deposit and the next withdrawal is four hours. This is significantly faster than the average of 40 hours for accounts that did not have an empty envelope transaction. The relationship also holds when examining the median time between transactions.

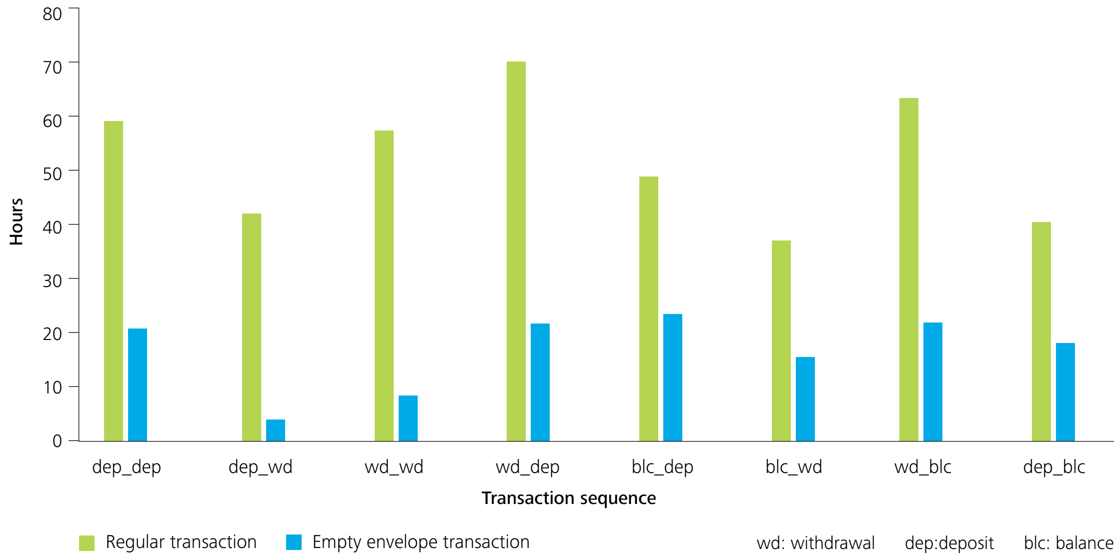
The average elapsed time across all transaction types associated with empty envelope deposit accounts is shorter than for all other accounts. We also observed that in a calendar week, accounts associated with empty envelope deposits had more than twice the number of withdrawals.

Based on this behavioural profile, the team derived eighteen features within the transactional data set to be used as potential inputs to regression and classification models. We adopted a regularized regression technique, the "elastic net," implemented using a coordinate-descent algorithm that achieves results in an order of magnitude less time than other methods[7].

The Bayesian interpretation of the elastic net technique further illustrates its power and flexibility: depending on the level of correlation present in the underlying data features, the user can vary prior distributions for model coefficients from normal (ridge- regression) to double-exponential (lasso regression). Large coefficients are penalized to avoid over-fitting, and under the double-exponential prior, irrelevant coefficients can be eliminated, thus simplifying the final model.

Preliminary results obtained using the set of eighteen derived features showed that the elastic net, used as a tool for regularized logistic regression, holds great potential in identifying empty envelope deposits.

Figure 3 – Average time between ATM transactions



Intelligent fraud management systems

It's not enough to rely on black box software and hardware solutions that purport to handle the putative data load; addressing fraud and corporate security in general, demands a combination of domain-specific expertise (certified fraud examiners, investigative professionals) and scientifically-focused personnel. Statisticians, computer scientists and fraud investigators can apply and further develop the latest research on data-driven monitoring algorithms.

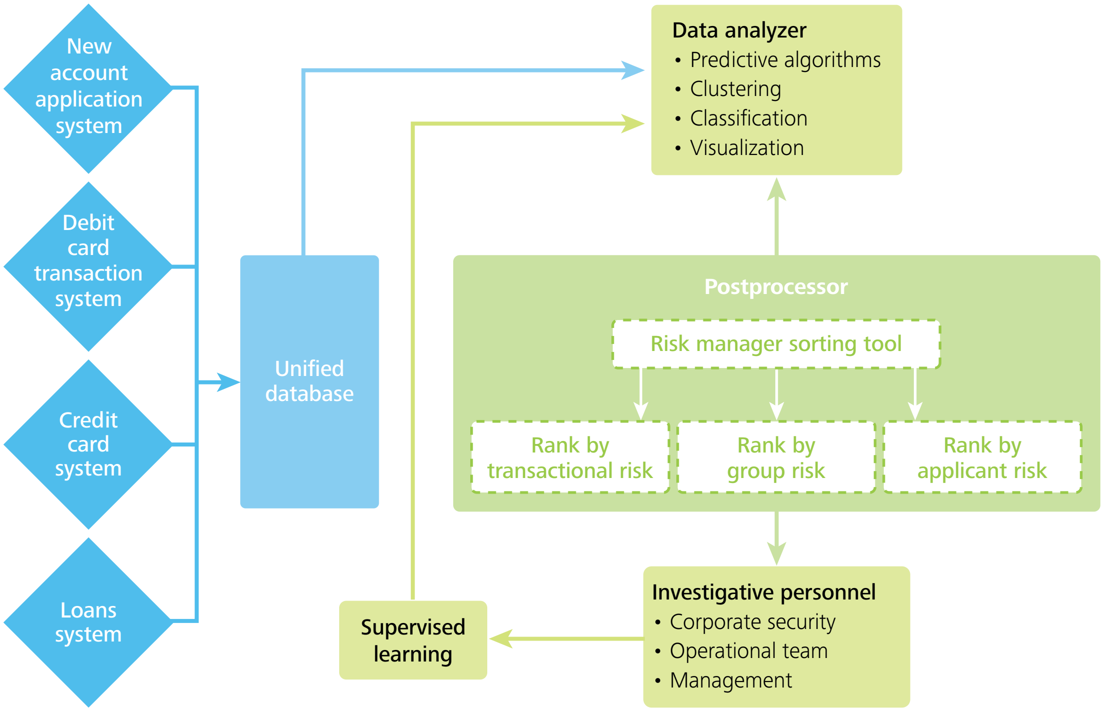
A recent survey of scientific literature[8] examines the latest financial fraud detection methods across a range of categories, including credit card fraud, money laundering and insurance fraud. Adaptive methods such as Bayesian Belief Networks and Hidden Markov Models are gaining prevalence due to their ability to rapidly update states of belief (i.e., was a given customer behaving fraudulently or not) based on the arrival of evidence (viz., any new transactional or other customer-related information).

When integrated closely with an existing transaction processing system, these methods can inform a parallel risk management layer for alerting and reporting purposes.

Account applicant risk scoring and behavioural risk monitoring are individual components that can reside within a unified framework of fraud management. The following sections present a high-level overview of one such potential framework.

In Figure 4, transactional, account and personal data are stored according to product type in disparate systems across the bank. The integrated fraud analysis system collates relevant attributes from external sources. The information can then be analyzed using enterprise-level data mining software to uncover hidden information. Examples include customer transactional behaviour, client groupings and similarities with respect to known fraud topologies. New clients can be assessed by comparing them against profiles of current and divested clients.

Figure 4 – Integrated fraud analysis system



Adaptive improvement to the fraud management system occurs through supervised learning, whereby results obtained from human investigators are fed back into the analysis.

Data mining tools that are effective in risk-ranking system-level entities such as clients and accounts include predictive algorithms, outlier detection, clustering, classification and visualization. These techniques will require specialized implementation and operational expertise as the demand for real-time analysis grows.

Adaptive improvement to the fraud management system occurs through supervised learning, whereby results obtained from human investigators are fed back into the analysis.

Account applicant risk scoring

The decision model for prioritizing risky applications for review (Figure 2) is contained within the fraud management system as a stream of analysis. New account application information is typically stored in a database that is isolated from other business units in the bank. When the applicant data is enriched with other data stores, complex patterns of activity can be uncovered. Data mining facilitates discovery of these patterns and identifies potentially risky customers for prioritized investigation by operational staff.

Behavioural risk monitoring

Relying on historical and current client transactions, the behavioural risk monitoring system is a stream of analysis that sits within the larger system (Figure 4). This information is combined with personal data and account attributes (tenure, type, overdraft conditions, etc.) to gain understanding of client behaviour. The data can be mined for hidden information such as behavioural patterns and correlations by grouping accounts by type, demographics and other attributes. In this analysis stream, client accounts are ranked and investigated by the operational team.

Making a difference through advanced analytics

The fraud landscape is ever evolving, and financial institutions must take ongoing measures to mitigate risk and stay secure. With recent changes to deposit legislation increasing empty envelope deposit fraud losses, banks face the need, and the opportunity, to augment their current fraud management systems with advanced analytics.

In collaboration with a large Canadian bank, Deloitte has confirmed that advanced analytics can provide insight on fraudulent behaviour that was not otherwise available. Preliminary analysis of reported empty envelope incidences revealed that perpetrators execute successive deposits and withdrawals over ten times faster than regular account holders, and this is only one of several predictors that could be used to identify risky individuals before they commit fraud.

The joint team then performed an in-depth analysis of the account application and transaction monitoring processes. After deriving model attributes using empty envelope transaction data, we identified ways to augment existing systems through a unified fraud management framework that employs applicant risk ranking and transactional behaviour monitoring.

The proposed solution not only fits seamlessly within existing fraud management frameworks, it can be applied across a range of financial institutions, putting predictive analytics front and center in the ongoing war against fraud.

The proposed solution not only fits seamlessly within existing fraud management frameworks, it can be applied across a range of financial institutions, putting predictive analytics front and center in the ongoing war against fraud.

Our team

Clayton Knight
Senior Manager, Financial Advisory
clknight@deloitte.ca
604-640-3146

Bryan Richardson
Manager, Financial Advisory
brrichardson@deloitte.ca
416-775-7335

Andrew Keats
Senior Consultant, Financial Advisory
akeats@deloitte.ca
416-775-4703

Endnotes

1. Cressey, 1953
2. Javelin Strategy & Research, 2012
3. Association of Certified Fraud Examiners, 2012
4. Items deposited that are later returned due to empty envelopes (Taylor-Butts, 2009). Throughout this paper, we adopt the terminology 'empty envelope deposit' to refer to worthless deposits made at ATMs or in person at bank branches.
5. Taylor-Butts, 2009
6. Government of Canada, 2012
7. Friedman, 2010
8. Ngai, Hu, Wong, & Chen, 2011

References

1. Association of Certified Fraud Examiners. (2012). *Report To The Nations on Occupational Fraud and Abuse.* Austin: Association of Certified Fraud Examiners Inc.
2. Canadian Bankers Association. (n.d.). *Credit Card Fraud and Debit Card Fraud Statistics – Canadian Issued Cards (2010 – 2011)*. Retrieved March 16, 2013, from Canadian Bankers Association: http://www.cba.ca/contents/files/statistics/stat_creditcardfraud_en.pdf
3. Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement.* Free Press Glencoe, IL.
4. Friedman, J. T. (2010). Regularization paths for generalized linear models via coordinate descent. *Journal of statistical software*, 33 (1).
5. Government of Canada. (2012, March 2). Access to Funds Regulations. Retrieved April 16, 2013, from Justice Laws Website: http://laws-lois.justice.gc.ca/PDF/SOR-2012-24.pdf
6. Javelin Strategy & Research. (2012). *Identity Fraud Report.* Pleasanton, California.
7. Merriam-Webster. (n.d.). *Merriam Webster.* Retrieved April 16, 2013, from http://www.merriam- webster.com/dictionary/fraud.
8. Ngai, E., Hu, Y., Wong, Y., & Chen, Y. a. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems,* 559-569.
9. Taylor-Butts, A. (2009). *Fraud Against Businesses in Canada: Results from a National Survey.* Ottawa: Statistics Canada.

www.deloitte.ca

Designed and produced by the Deloitte Design Studio, Canada. 13-3516