****

9b17e005

rbc: social network analysis

R. Chandrasekhar wrote this case under the supervision of Professor Peter Bell solely to provide material for class discussion. The authors do not intend to illustrate either effective or ineffective handling of a managerial situation. The authors may have disguised certain names and other identifying information to protect confidentiality.

*This publication may not be transmitted, photocopied, digitized, or otherwise reproduced in any form or by any means without the permission of the copyright holder. Reproduction of this material is not covered under authorization by any reproduction rights organization. To order copies or request permission to reproduce materials, contact Ivey Publishing, Ivey Business School, Western University, London, Ontario, Canada, N6G 0N1; (t) 519.661.3208; (e)* [*cases@ivey.ca*](mailto:cases@ivey.ca)*;* [*www.iveycases.com*](http://www.iveycases.com)*.*

Copyright © 2017, Richard Ivey School of Business Foundation Version: 2017-06-13

In October 2013, Daniel McKenzie was reviewing the mandate of his first-of-its-kind new role at the Royal Bank of Canada (RBC), Canada’s largest bank. Reporting to the bank’s vice president (Fraud), McKenzie had been appointed as head of Enterprise Fraud Strategy, a department tasked with protecting RBC’s global customers from fraud.

McKenzie’s immediate priority was to prevent fraudulent transactions by RBC’s own customers—a phenomenon called first-party fraud—by implementing a bourgeoning technology called social network analysis (SNA). The technology used predictive analytics to forecast the occurrence of first-party fraud. McKenzie reflected,

As we begin to deploy predictive analytics in preventing first-party fraud at RBC, I am facing three managerial dilemmas. First, how should SNA be used to bring down the ratio of fraud alerts to actual frauds at RBC? [As of October 2013,] the incidence of false positives, as they are called, [is high] at 85:1. We must bring it down to 10:1. Second, how should the cost of maintaining SNA protocols be reduced? SNA is characterized by data intensity. The process of extracting, transferring, and loading large data sets (known as ETL) is expensive. We have to strike a balance between fraud loss avoidance and operational efficiency. Finally, how should the issues around systemic performance of SNA be resolved? We should reduce the time lag with ETL processes and make ETL real time.

RBC

Established as Merchant’s Bank of Halifax in 1869 and renamed the Royal Bank of Canada in 1901, RBC was Canada’s largest bank as measured by assets and market capitalization. The bank was also the largest card issuer in Canada, with 6.5 million cards. It had about 80,000 full- and part-time employees and served more than 15 million clients in Canada, the United States, and 49 other countries.

RBC was driven by a vision of “earning the right to be our clients’ first choice.” The bank was pursuing this vision through three strategic goals: (1) to hold on to the leadership position in financial services in Canada; (2) to provide capital market and wealth management solutions outside Canada; and (3) to offer, in targeted markets, products and services complementary to its core strengths. The bank’s strategy for growth and profitability had remained consistent over the years, while its structure was being fine-tuned regularly.

In October 2012, RBC had restructured its business into five segments: personal and commercial banking (meeting the banking needs of individuals and businesses), wealth management (serving high-net-worth individuals), insurance (offering insurance and reinsurance products through various channels), investor and treasury services (serving the needs of institutional clients), and capital markets (comprising global wholesale banking). These five business segments were supported by two streams: technology & operations (forming the technological and operational bedrock for the organization) and functions (including finance, human resources, risk management, corporate treasury, and internal audit). McKenzie explained,

We have four objectives at RBC with regard to fraud prevention: reducing losses; enhancing customer experience, lowering costs; and minimizing overall risk. In balancing these objectives, we have given high weighting to enhancing customer experience in two ways. We have converted areas of potential customer inconvenience into areas of customer care. It is mandatory in every . . . wire transaction, for example, for a bank to make telephonic enquiries with the home branch, which in turn calls up the sender with specific questions to confirm the veracity of the transaction. Invariably, the protocol causes processing delays, often hours. The information would also fall short of requirement. What we have done at RBC is to set up a dedicated team to call the sender directly, within minutes. Customers appreciate such calls. The resolution time has come down from an average of two hours to less than 20 minutes. Secondly, we look for customer service opportunities in deploying fraud solutions. We have leveraged big data to provide a snapshot of each customer to the call centre to make [customers] feel better about offers made during the conversation, fulfilling specific needs.

RBC had more than six million customers, but it was conservative about who it lent money or granted credit cards to. The core anchor of RBC’s fraud prevention program was the service reference file (SRF), which was specific to each individual customer. Each SRF provided multiple frames of reference as it unfolded progressively over the life cycle of an RBC customer. Before the bank introduced SNA, fraud detection fell under the domain of the bank’s Corporate Investigations Services (CIS) division. CIS was similar to an internal police service but had other ongoing responsibilities as well, like offering protection services for the bank’s senior executives. There was a dollar threshold to be met before the CIS could intervene in a fraud investigation. The CIS would interview the suspects and build a case for prosecution while RBC would “demarket” a customer proven to be indulging in fraudulent transactions.

FIRST- AND THIRD-PARTY FRAUD

In general, a banking fraud had five characteristics. First, it was uncommon: the number of fraud cases in a data set was small, usually less than 1 per cent, rendering the data set imbalanced and making it difficult to achieve predictive accuracy. Therefore, it was necessary to reconfigure the data in a bid to restore balance and make it work, and this was usually done by over-sampling the minority class or under-sampling the majority class.[[1]](#footnote-1)

Second, each fraud was preceded by a well-considered plan of action and was never ad hoc. Third, fraud was not an individual phenomenon; it was invariably the result of a networked organization. Fourth, fraud was typically concealed so well that it would not be noticed until after it had been committed and so required expert intervention for detection. Finally, fraud methods evolved over time, meaning that the detection experts were always trying to catch up with the latest techniques.

The two main types of fraud were first-party fraud and third-party fraud. Third-party fraud happened when a third party stole the identities of honest/legitimate RBC customers and used these identities to steal money both from the customer and the bank. Third-party fraud was difficult to detect because fraudsters went to great lengths to seem like those they were pretending to be. The account was usually put through the conventional collections treatment to be written off, over time, as bad debt. Third-party fraud was subject to a fuller investigation because it was officially classified as fraud (unlike first-party fraud).

First-party fraud occurred when customers applied for credit cards, loans, overdrafts, or unsecured lines of credit with a clear intent to swindle their own bank. Their applications would be backed by a good credit history, built by conscious design over several years (through well-orchestrated moves like making regular payments from their accounts, and purchasing high-profile products from the bank, such as property insurance).

During the period of build-up, the fraudsters would also use a technique called “cash cycling,” wherein they would create an illusion of legitimacy by circulating amounts at intervals among several other accounts, both within their own bank and at other banks. The accounts would all be part of a fraudulent network, sharing some common data elements (like name, date of birth, phone number, address, Social Insurance Number, etc.). The account behaviours would be normal and would therefore pass through conventional customer analytics without raising any red flags. Once they secured sufficient lines of credit, however, the customers would “bust out” within days, purchasing high-priced goods and withdrawing cash from various accounts that would be seemingly disparate but interconnected.

McKenzie described the disastrous effects of first-party fraud:

A unique feature of first-party fraud is the exponential nature of the relationship between the number of fraudsters and the overall dollar value being defrauded. Ten fraudsters sharing 10 common data elements can create 100 false identities; and if they defraud four financial instruments per identity, each with a CA$5,000[[2]](#footnote-2) credit limit, the potential loss to the financial system would be $2 million. This ability, known as connected explosion, is a source of strength for organized crime involved in first-party fraud, but, it is also its Achilles’ heel. It is their connectivity that renders first-party fraudsters vulnerable to modern fraud detection tools like SNA, which leverages the very connectivity that is the basis of first-party fraud.

National estimates of the magnitude of first-party fraud were not readily available because first-party fraud was not officially classified as fraud, although the value of consumer credit being written off as bad debt provided some indication. In the United States, for example, the Federal Reserve System reported that out of US$850 billion outstanding in revolving consumer credit, US$85 billion was written off annually as uncollectible.[[3]](#footnote-3) Roughly 5 to 20 per cent (US$4 to US$17 billion) was misclassified as bad debt when it should have been categorized as first-party fraud.[[4]](#footnote-4)

In the United Kingdom, the British Bankers Association estimated that 10 to 15 per cent of bad debt losses incurred by the banking sector were from first-party fraud. The United Kingdom had a higher proportion of “transient” people—students, short-term workers—leading to a higher rate of “bust out” behaviour. Similarly, the value of receivables being written off by an individual bank provided a clue to the extent of first-party fraud among its customers within its own premises.

Financial fraud affected all stakeholders in the value chain to varying degrees. For instance, the Federal Bureau of Investigation had estimated that fraud cost U.S. insurers US$30 billion each year, and that, in turn, insurance fraud cost the average U.S. family between US$200 and US$300 per year in the form of increased premiums.

SOCIAL NETWORK ANALYSIS

SNA was defined as “the mapping and measuring of relationships and flows between people, groups, organizations, computers, URLs, and other connected information/knowledge entities.”[[5]](#footnote-5) The concept had its beginnings in the 1930s, as a metaphor for complex sets of relationships among members of a social system. In the 1960s and 1970s, SNA was positioned at the intersection of psychology, anthropology, sociology, organizational design, and mathematics.

The application of graph theory, in particular, enabled SNA’s evolution from suggestive metaphors to analytical models. SNA’s perspective of networks of human relationships and its provision for their visual and mathematical analysis enabled data scientists to make key assumptions about the frequency, quality, and expansive nature of interactions among individuals. A flow of money between two individuals was seen as evidence of a firm and clear link between them. McKenzie defined and described the role of SNA in detecting fraud:

At its simplest, SNA identifies interpersonal relationships among a group of individuals, and also provides a degree of evaluation (see Exhibit 1), but, it is different from social media networks like Facebook and Twitter. SNA focuses on interactions among customers of financial institutions. It enables financial institutions to examine collaborations of their customers, as individuals, by pooling information from multiple data elements. SNA picks up nuggets of information from seemingly unrelated data in order to identify motives of people with suspicious transactions, and pinpoint, for pre-emptive action, those on the verge of committing a fraud.

The volume of transactions flowing through banks was so huge that spotting evidence of fraud was usually like looking for the proverbial needle in a haystack. However, SNA was unique in the sense that it used a single uncovered needle to identify other needles in the haystack and expose rings or patterns of fraud.

SNA had its own terminology, consisting of nodes (representing persons, locations, or companies) and edges (establishing connection between two nodes). Each node was assigned a weighting in terms of the level of its crime, and each edge was assigned a weighting in terms of the intensity of its involvement. Because networks were very large, making it difficult to extract features from them, the focus of investigation was usually the neighbourhood of a network. There was also a distinction between first-order networks (comprising direct associates of a network) and N-order network (comprising all others).

The manner in which a network structure was represented was also critical. The link representing financial resources transferred between two nodes could be binary (attesting to the shared resource), absolute (stating the number of resources shared), or relative (stating it as a percentage). The visual representation was mapped to a matrix, with rows and columns, to make it easier for investigators to work with. Resources were represented as diamonds. Several sociological tests were deployed to convert network knowledge, however minimal, into a fraud detection tool; an example was “homophily,” a term borrowed from sociology, where it represented the tendency of people to associate with “people like themselves” (e.g., those from the same city or with common interests). In the context of fraud networks, homophily meant that fraudulent people were most likely to be connected to other fraudulent people. Data sets containing statistically significant patterns of homophily were called clusters, which, for that reason, were subject to closer scrutiny by investigators.

An important step in SNA was the extraction of features. The focus would usually be on the first-order “neighbourhood,” as RBC referred to it internally. It was known more generally as egonet. The neighbourhood (or egonet) had two components: the specific node of interest (known as ego) and its direct associates (known as alters). The features would be egonet-generic (measured through metrics like degree, relative degree, and triangle) and alter-specific (measured through metrics like similarity, fraud score, and weighted fraud score). The nodes were ranked in terms of fraud risk probability on lines similar to Google’s PageRank algorithm.

Because fraudsters were densely connected to one another, network models like SNA were known to perform better in terms of parameters like accuracy (by using skewed distribution as the basis to distinguish fraudulent customers), precision (by identifying potential high-risk customers from a long list), and recall (by detecting fraudulent customers).

FRAUD DETECTION ISSUES AT RBC

McKenzie identified several objectives in moving forward with fraud detection systems at RBC:

Lowering the False Positive Rate

When fully implemented, at the beginning of each week, the SNA system would provide McKenzie with a visual representation linking individual entities that would potentially perpetrate larger-scale frauds (see Exhibit 1). The system would also provide him with a percentage of claim alerts scoring high for fraud potential.

Attempts to identify fraudulent customers would sometimes lead to alerts that proved incorrect after further investigation (i.e., the customers were not fraudsters). As a result, the false positive rate (FPR), or percentage of alerts that were found to be honest customers was a key metric of any detection system. Lowering the FPR was critical in avoiding the expense of investigating false positives. If McKenzie received 85 alerts at the beginning of a week, and only one of them was actually a fraud perpetrator, the remaining 84 alerts resulted in a huge waste of time, money, and human investigative resources. Bringing down the FPR also meant focusing on the most “high-likelihood” cases. This focus was important because false positives created undesired side effects. The last thing a financial institution would want to do was chase off legitimate customers by considering them as potential fraudsters.

A fraud detection system was amenable to a high FPR because there was no customer interface. One possible solution to this issue was to replicate the model used by credit card systems, which had no provision for a high FPR because it had to approve or decline the transaction within seconds. The system had a direct interface with the customer, who would be waiting for closure of the transaction.

Reducing the Cost of the Analytics Systems

The analytics system had cost RBC $10 million upfront. The recurring annual costs of hardware maintenance were about $1 million, but the major cost element was due to the data intensity of the system. The system was processing 30 terabytes of data every week. The system had to find the data, make sense of it, extract the data, and format it in a way that was actionable; all of this was costly and time consuming, requiring dedicated resources in terms of both staff time and machine capacity.

McKenzie was considering two cost-reduction options in the long term. One was to store the data in the online server (cloud), but this option contrasted sharply with RBC’s traditionally conservative approach to protecting its customers’ data. It was unlikely that RBC would pursue this cloud approach unless the requirements of the technology were very strong. The second option (one that demonstrated RBC’s desire to embrace the latest technologies) was to outsource ETL; the limitation here was that the vendor ecosystem had not developed enough, and there were not many individual vendors with the scale that RBC required.

Resolving Issues around Systemic Performance of SNA

This objective was also linked to the issues regarding data acquisition. A giant server at the data centre of RBC had crunched data for five days straight, providing historical rather than real-time data. The slow pace of the batch-processing backend was in contrast to the frontend, wherein a potential fraudster did not have to wait for five days to get a credit card or open a new account. An alternative would be to run the analysis over the weekends (lasting for two days at a stretch) with incremental processing during four consecutive weeknights.

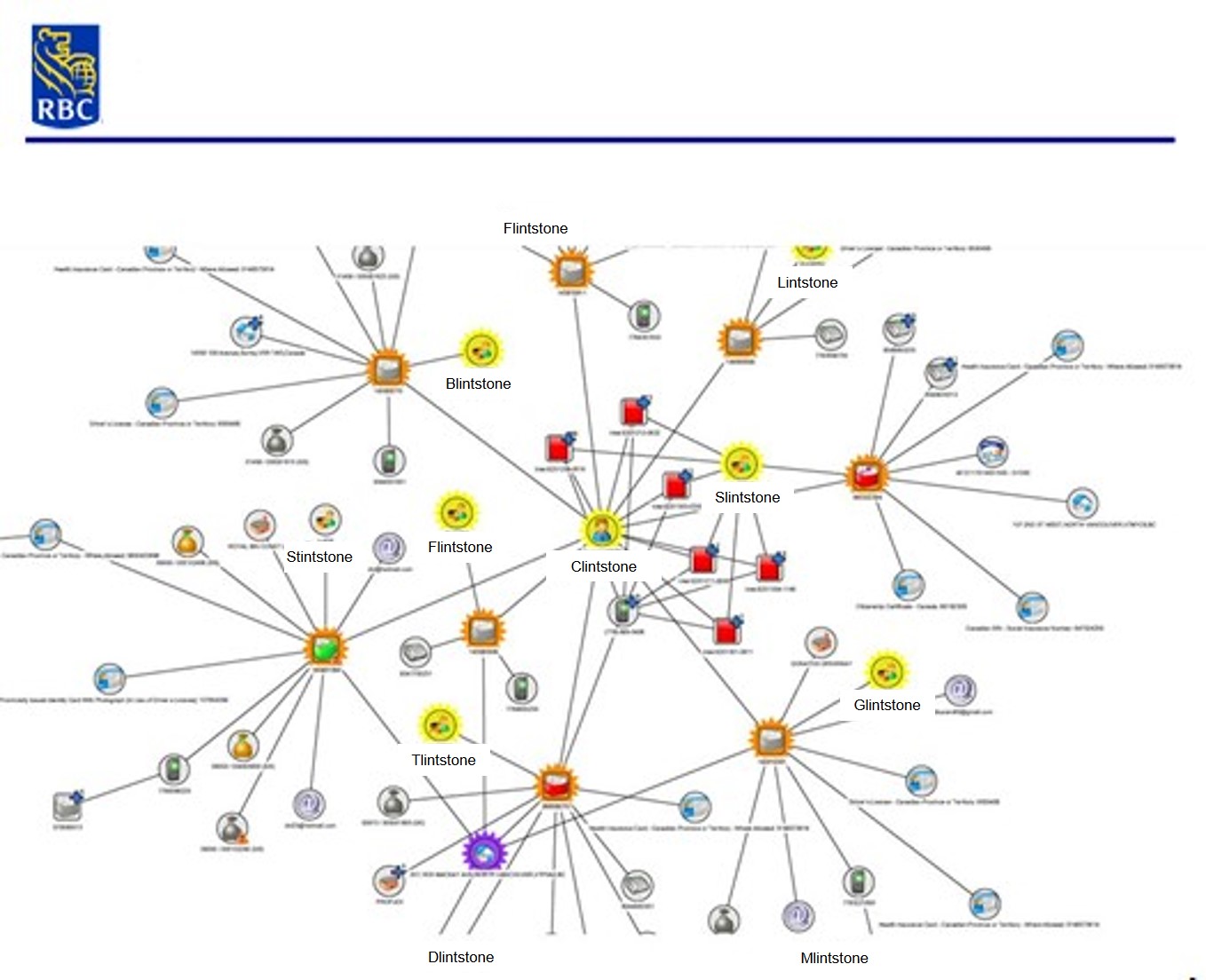
The second performance problem with SNA was the prevalence of what were known as “super clusters.” A super cluster was a formation in which everybody was linked to everybody else. A super cluster required frequent changing of entry thresholds so that the clusters were manageable. Every time there was a change, the network had to be run all over again. In a network of, for instance, one million, there were bound to be frequent changes in composition.

NEXT STEPS

Fraudsters were currently being detected using rule-based logical searches. A customer was selected, and the pattern of that customer’s financial transfers to other RBC accounts was investigated by applying rules that searched for internal transactions that would reveal the types of networks illustrated in Exhibit 2. The complexity of the rules required the detection of complex networks, and the large number of RBC accounts made executing the rules through the RBC customer database a prodigious data-processing task.

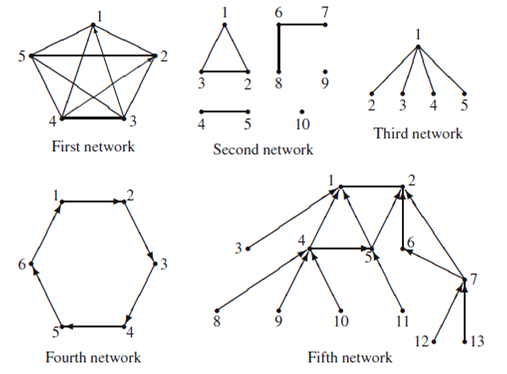
In considering his next steps, McKenzie decided to look at the data from a recent analysis. This historical analysis was summarized in an Excel spreadsheet, where 16 fraud detection rules had been applied to 13,731 customers who had been found to be “fraudsters” or “not-fraudsters” following extensive further investigations. McKenzie was interested in finding out which rule, or combination of rules, provided the best fraud detection and how effective this rule (or combination) would be if implemented for all RBC customers. Since applying even a single rule was very time consuming and costly, it was also important for McKenzie to know if he could discard some rules as ineffective.

Exhibit 1: SOCIAL NETWORK ANALYSIS



Source: Company files.

Exhibit **2: TYPES OF NETWORKS**



Note: The above diagrams provide five hypothetical social networks involving a small number of nodes to illustrate some of the wide variety of networks possible. The first network, involving five nodes, is close to the situation where everybody goes to everybody else. In the second network, involving 10 nodes, the ties are all reciprocated but the network is highly fragmented. The third network, comprising five nodes, is connected but shows a concentration of power. It is held together by a single node whose disappearance will disintegrate the network. The fourth network, involving six nodes, is also connected in the sense that everybody can go to everybody else—but through a large number of intermediaries. The fifth network, involving 13 nodes, displays a strong hierarchy, and although it is connected, the ties flow in only one direction.

Source: David Knoke and Song Yang, *Social Network Analysis*, 2nd ed. (Los Angeles, CA: Sage Publications, 2008).

1. The most commonly used technique was the synthetic minority over-sampling technique (SMOTE); Nitesh V. Chawla, Kevin W. Bowyer, Lawrence O. Hall, and W. Philip Kegelmeyer, “SMOTE: Synthetic Minority Over-Sampling Technique,” Journal of Artificial Intelligence Research 16 (2002): 321–357. [↑](#footnote-ref-1)
2. All currency amounts are in Canadian dollars unless otherwise specified. [↑](#footnote-ref-2)
3. The Federal Reserve Bank, “Federal Reserve Statistical Release: Net Charge-off and Delinquency Rates on Loans & Leases at Commercial Banks,” Q1 2010 Web, June 30, 2010, accessed May 12, 2015, www.federalreserve.gov/datadownload. [↑](#footnote-ref-3)
4. Dale Daley and Rod Powers, “Recognizing First-Party Fraud: Why It’s More Expensive Than You May Think,” TSYS, 2011, accessed July 15, 2015, http://tsys.com/Assets/TSYS/downloads/wp\_recognizing-first-party-fraud.pdf. [↑](#footnote-ref-4)
5. Valdis Krebs, “Social Network Analysis: An Introduction,” Orgnet, accessed December 8, 2016, www.orgnet.com/sna.html. [↑](#footnote-ref-5)