Machine Learning with Applications 8 (2022) 100269

Contents lists available at ScienceDirect

Machine Learning with Applications

journal homepage: www.elsevier.com/locate/mlwa

Fraud prediction using machine learning: The case of investment advisors in Canada

Mark Eshwar Lokanan *, Kush Sharma

Faculty of Management, Royal Roads University, T 250.391.2600 ext. 4386#, 2005 Sooke Road, Victoria, BC, Canada V9B 5Y2

ARTICLE INFO

Keywords:
Fraud
Machine learning
Financial markets
Regulation

ABSTRACT

The paper contributes to a growing body of empirical work on regulatory technology by proposing machine learning models to detect fraud in financial markets. The recent spate of investment fraud in Canada has exposed regulators' inability to protect vulnerable investors and the financial markets from financial abuse. As evident by the numerous regulatory task force commissioned in the past two years, Canadian regulators have been looking for ways to detect and prevent fraudulent activities before they occur and support enhanced enforcement powers. The purpose of this study is to use data collected from the Investment Industry Regulatory Organization of Canada (IIROC) to build a machine-learning algorithm to predict fraud in the Canadian securities industry. Data for this project were collected from IIROC's tribunal cases covering June 2008 to December 2019. In total, 406 cases were retrieved from the IIROC's website. The results from four machine learning models reveal that across all the features, the amount of money invested and whether the offender was from a bank-owned investment firm were the high predictors of fraud in terms of the standardized coefficient. Branch managers and regulators should pay careful attention to portfolios that continuously incur losses as a sign of potential fraud. The findings are particularly relevant to regulators seeking new and effective fraud detection techniques while providing enhanced clarity to Canada's financial markets' self-regulation.

1. Introduction

"Crime Without Punishment: Canada's Investment Fraud Problem" (Gray & McFarland, 2013); "Easy Money: How Fraudsters Can Make Millions Off Canadian Investors, Get Barely Punished and Do It Again" (Robertson & Cardoso, 2017); "2 Men Charged in Multi-Million Dollar Investment Fraud: Lethbridge Police" (Knight, 2020); and "90-Year-Old RBC Client Allegedly Lost $60K to Fraud by Longtime Advisor" (Alini, 2020). These headlines highlight the magnitude of Canada's investment fraud problem, raise concerns over capital market regulators' ability to detect suspicious activities before they occur, and illustrate their inability to protect individuals vulnerable to fraud. The Canadian Securities Administrators, in a recent report, noted that fraud detection is a serious problem for Canadian regulators and encouraged them to raise their profiles and find more innovative ways to detect issues earlier (2020). Regulators owe it to Canadians to do a better job of protecting them from investment fraud. One such regulator is the Investment Industry Regulatory Organization of Canada (IIROC)—Canada's national self-regulatory organization (SRO) responsible for policing its debt and securities markets.[1]

The IIROC has been criticized by investors' advocate for not being able to regulate in the public interest (Canadian Foundation for Advancement of Investor Rights (Fair Canada, 2014; Lokanan, 2019). At the root of these criticisms is the IIROC's inability to work with dealer members to detect red flags for fraud before it occurs. Part of the problem is its archaic enforcement system that requires complaints to be reported by dealer firms and by the IIROC rather than allowing the IIROC to work with its members to detect the potential for fraudulent events before they occur. A recent report by the Capital Markets Modernization Taskforce (hereafter referred to as Taskforce) on financial market regulation in Canada encouraged the IIROC to use computational intelligence to improve its fraud detection and prevention efforts (Soliman et al., 2011).

For the IIROC, maintaining safe and efficient capital markets is fundamental to its legitimacy as a gatekeeper in Canadian finance. Although these duties are typically taken for granted, the recent spate of investment fraud in Canada has led to intense scrutiny of the IIROC. In this paper, investment fraud is contextualized as a purported attribute of financial markets undergirded by deceit and manipulation. This study shifts the grounds of the discussion from the efficiency of the

* Corresponding author.
E-mail addresses: Mark.Lokanan@royalroads.ca (M.E. Lokanan), sharmakush03@gmail.com (K. Sharma).
URL: http://royalroads.ca (M.E. Lokanan).

[1] The other SRO that plays a vital role in regulating Canada's capital market is the Mutual Funds Dealer Association of Canada (MFDA). The MFDA is the national SRO that regulates mutual funds dealers in Canada.

https://doi.org/10.1016/j.mlwa.2022.100269
Received 8 August 2021; Received in revised form 24 January 2022; Accepted 24 January 2022
Available online 31 January 2022

IIROC in regulating the financial markets to one that exposes the fault lines of the attributes that lead to fraud. Rather than using traditional selection methods to identify red flags of fraud, the IIROC and dealer members can use machine learning techniques to detect fraud more effectively – with high predictive accuracy – from large unstructured data sets. Adopting the Taskforce's directive that the IIROC needs to improve its fraud detection efforts, in this paper we examine the following two research questions:

1. How does the probability of investment fraud vary within categories of victim and offender demographics?
2. What features are the strongest predictors of investment fraud?

In answering these questions, I make two contributions to the financial regulatory literature.

First, this paper has implications for all the key players in Canada's capital markets. The findings are of first-order importance to the following: regulators because they design policies to protect the public interests, investment firms striving to improve compliance with regulators and bolster investor relations, and retail and institutional investors who need assurance that regulators are equipped to ensure safe and strong capital markets. In this way, I contribute broadly to the financial market regulation scholarship and specifically to the feasibility of self-regulation in finance.

Second, machine learning algorithms have been used extensively by researchers in business, computer science, engineering, and the medical field to predict future events. With the recent increase in fraudulent activities in Canada's financial markets, machine learning could play a pivotal role in predicting and spotting red flags for fraud. However, although machine learning has been used to predict credit card and financial statement frauds, loan defaults, and money-laundering transactions, no researchers to date have employed machine learning to predict fraud in financial markets (Duman & Ozcelik, 2011; Perols, 2011; Perols et al., 2017; Sahin & Duman, 2011). By introducing a novel machine learning technique into the process of financial market regulation, I contribute to the scholarship on critical fraud research.

The rest of the paper proceeds in four sections. In the first section, I describe the theory of self-regulation and survey the existing literature on the use of self-regulatory systems in financial markets. In section two, we describe the methodology, with particular emphasis on the machine learning approach and algorithms employed in the models. In section three, I discuss the results of the findings and argue the key role that machine learning algorithms can play in modernizing SROs' enforcement and fraud detection in financial markets. In the final section, I conclude with a brief discussion on the implications of SROs in regulating financial markets and highlight future areas of research for machine learning in regulatory scholarship.

2. Self-regulation and financial market regulation

2.1. Criticisms of self-regulation

Self-regulation in financial market governance is rooted in the neoliberal policies of deregulation, liberalization, and privatization (Emeseh et al., 2010, p. 232). The deregulative approach to financial market governance has led to the dismantling of state power, which has thus given SROs more freedom and an active role in financial market activities (Braithwaite, 2013; Lokanan, 2015). Government intervention is only needed when SROs fail to regulate in the public interest or hold their members accountable to laws and ethical standards (Brockman, 2004).

The effectiveness of self-regulation has been debated by policymakers since the onset of neoliberalism, when private sector models such as self-regulation were implemented by industry leaders to inspire economic development (Baggot, 1989; Devlin & Cheng, 2010; Paton, 2008; Rees, 2013). Given that the costs are borne by the market itself, a system of self-regulation is more cost-effective than government regulation (Lokanan, 2015). By virtue of being closer to the action, some experts consider self-regulation to be faster and more flexible than government regulation because of the ability of industry experts to identify regulatory "hot spots" of fraud (Linhart, 2017; Lokanan, 2017; Williams, 2012). SROs have the potential to use industry insiders to "funnel in" more cases that otherwise would go unaccounted for in government regulation (Brockman, 2004; Lokanan, 2015). Nonetheless, experts are divided on whether self-regulatory systems work to safeguard the public interest or only their members (Lokanan, 2015).

Notably, *public interest* has not been explicitly defined in the regulatory literature. In most accounts, the definition of public interests draws on themes that are invariably accorded a privileged place with limited frames, shaped by the views of dominant special interest groups (Kuhlmann et al., 2009; Paton, 2008). By depoliticizing financial markets as natural places where buyers and sellers have an equal chance to be successful in the purchase and sale of goods and services, some accountants have limited the conceptualization of public interest to either consumer interests and cost of service or resource accessibility (Kuhlmann et al., 2009; Paton, 2008). Others view public interests as more systematic expressions of social values – such as justice, freedom, public safety, and general welfare – that cannot be excluded in the evaluation of SROs' effectiveness in financial market regulation (Dixon-Woods et al., 2011; Kuhlmann & Saks, 2008). Because the scope and meaning of the term are contested in the literature, what translates to the public good for specific groups does not necessarily uphold society's best interests. Numerous studies have shown that self-interest plays an important role in financial market regulations, even if the arguments for self-regulation are genuinely framed in the public interest (Devlin & Cheng, 2010; Lokanan, 2018; Yokoi-Arai, 2007). A key point to consider in the analysis of self-regulation is that as the financial market expands, so too does SROs' financing and the cost of engaging in self-enforcement (Tarbert, 2021).

2.2. The arguments for self-regulation

Despite these criticisms of SROs' governance of the financial markets, some believe that the advantage of self-regulation can be realized if member firms are willing to comply with self-regulatory systems (Braithwaite, 2013; Heath, 2018; Lokanan, 2018). For self-regulatory systems to be effective in finance, a collective action by industry participants to ensure compliance is necessary (Garvie, 1999; Shiell & Chapman, 2000; Sinclair, 1997). Some benefits accrued by individual compliance can be private in nature, but many are external to the firm and can work to create a culture of compliance in the industry as a whole (Garvie, 1999; Klassen & Whybark, 1999).

Along these same lines of responsibility, regulatory experts argue that SROs will enforce regulation to the extent that they can ward off direct government intervention (Baggot, 1989; Brockman, 2004; Lokanan, 2019; Sinclair, 1997). Statutory intervention is considered more expensive and disruptive for firms (Baggot, 1989; Sinclair, 1997). Through these lenses, industry self-regulation appears a charade—an appearance of effective regulation through which government finds an excuse to shed itself of the responsibility for regulating the financial markets (Braithwaite & Fisse, 1987). This understanding of regulation and the markets informs the position of both proponents and opponents of self-regulation. For the former, self-regulatory systems – despite their flaws – are necessary to act as impartial umpires and control the irrational exuberance of the markets. For the latter, self-regulation is perceived as a zero-sum game in which increased government intervention translates to decreased efficiency and economic fluidity.

Among the myriad changes to affect financial market regulation, technological advancements in the field of big data offer opportunities for improved surveillance (Hildebrandt, 2018; van Liebergen, 2017; Williams, 2013). The sociotechnical ensemble and growth of computational intelligence over the past decade have enhanced the processing power of machines to conduct predictive analytics that human cognition could not have otherwise recognized or detected (Cohen, 2012; Yeung, 2018). Through the use of computational intelligence,

regulatory technology proactively scans financial markets' data for red flags and then feeds the results to its human counterparts, who then uncover hidden patterns and make informed decisions (Narang, 2021; van Liebergen, 2017; Wall, 2018; Williams, 2012). The Taskforce's (2021) report to the Ontario Minister of Finance on the Capital Markets Modernization in Canada reinforced this last point, noting that regulators must reflect the market realities of today and use computational intelligence to ensure that "market participants comply with securities laws" and protect investors from market abuse (Soliman et al., 2021, p. 87). It is within this context – the contemporary context of financial market and securities regulation – that machine learning can play a useful role.

2.3. Machine learning and prior fraud prediction research

Machine learning is an emerging field in fraud prediction research. Authors of empirical studies on fraud prediction have employed supervised learning algorithms to enhance the general understanding of fraud prediction (Perols et al., 2017; Severina & Peng, 2021). Researchers on financial statement and credit card fraud detection, for example, have used machine learning algorithms to classify the incidence of fraud and non-fraud transactions (Lokanan, 2019; Phua et al., 2010). Research on fraud classification models have employed artificial neural networks (ANNs), Bayesian networks, decision trees, ensembles, rule-based systems, fuzzy theory, and support vector machine (SVM) algorithms to classify the incidence of fraud and improve fraud prediction in various domains (Bhatia et al., 2016; Bhattacharyya et al., 2011; Osegi & Jumbo, 2021; Perols et al., 2017; Severina & Peng, 2021; Vlasselaer et al., 2016).

Early and more recent research on fraud prediction have noted that ANNs perform significantly better than discriminant and accounting ratio-based logistic regression algorithms (Beneish, 1999; Perols et al., 2017; Summers & Sweeney, 1998). More recently, researchers have employed ensemble-based and decision tree algorithms to detect financial statement and management fraud (Hajek & Henriques, 2017; Perols, 2011). Other scholars using advanced machine learning algorithms such as SVM have found that they outperform traditional logistic and ensemble-based methods in predicting accounting fraud (Cecchini et al., 2010; Perols, 2011; Perols et al., 2017; Severina & Peng, 2021). However, this body of work, rooted in using accounting ratios as independent variables to predict fraud, should be interpreted with caution because accounting data are notorious for being highly unreliable and, more importantly, there is no universally accepted model for all data types (Fernández Delgado et al., 2014). When making causal inferences, researchers should keep in mind that there is no universal best model for all data types, and when making comparisons, every algorithm should be evaluated independently from its competitors (Hoggett et al., 2019).

Recent researchers have found that discriminant analysis and logistical regression are the most deployed algorithms in credit card fraud prediction because of their simplicity, lower computational costs, and ability to detect anomalies with smaller sample sizes (Campus, 2018; Kaminski & Guan, 2004; Osegi & Jumbo, 2021; Pai et al., 2011). Adopters of other methods such as ANNs have employed fuzzy systems to identify fraudulent credit card transactions with accurate results (Osegi & Jumbo, 2021; Sahin & Duman, 2011). Evidently, although most researchers to date have employed various machine learning and neural networks algorithms to predict fraud, none to date have employed these algorithms to predict fraud in financial market transactions. In this paper, we have attempted to fill this gap by employing machine learning algorithms to predict investment fraud in the securities market. In so doing, this paper adds to an emerging stream of literature that examines classical machine learning to improve fraud prediction.

3. Research methodology

3.1. Data collection and sample

As is evident from the literature review, classification problems have suffered from uneven distribution among classes, yet they are considered important problems in fraud detection that uses machine learning in several domains (Whiting et al., 2012). This study is in one of those domains. Data for the study came from the IIROC's tribunal cases. The IIROC was formed in 2008, and we collected data from the period between June 2008 and December 2019. The primary data came from the enforcement cases on the IIROC's website. In total, we retrieved 406 cases from the IIROC's website and coded them into a CSV file. Rather than selecting a sample of cases, we uploaded the entire population of cases on the IIROC's website heard by a hearing panel between 2008 and 2019. We preferred this data collection strategy for two fundamental reasons. First, using only a sample of the data could have resulted in studying cases that had little to offer in terms of data granularity. Second, a sample of the cases could have included more cases from the larger Canadian provinces at the expense of the smaller provinces. Consequently, it was methodologically more useful to code all cases from the IIROC's database.

3.2. Coding of data

We used two rounds of coding to code the cases. The first round of coding involved a pilot of 20 cases. We selected the cases to represent all the IIROC's district councils across Canada. During the first round, we wanted to discover the type of input features that can be used to predict fraud. The first round was beneficial because it allowed us a better understanding of the type of data available and how to structure and frame it in the Excel database. In the first round, we collected data on victims, offenders, and enforcement attributes. Once we felt we had a comprehensive understanding of the data, the principal investigator then trained two research assistants (RAs) to assist with coding the entire data set. To avoid confusion, the principal investigator assigned each RA a different set of attributes to code—RA 1 received victims' attributes, and RA 2 received offenders' attributes. Data on victims' attributes included the number of investors, the amount of money lost, the amount of money invested, the gender and age of the victim, the liquid assets of the victim, their employment status, their relationship to the offender, and their investment knowledge. Data on offenders' attributes include the district council they were from, the commission they earned, their occupation, their disciplinary history, the type of firm they belonged to (bank-owned or private investment; retail or institutional), their experience in the industry, and their gender. Once we had collected all data, we combined both Excel files into one data frame using Pandas.[2]

3.3. Predictor variables and measurements

3.3.1. Independent variables

The independent variables consisted of several victim- and offender-related features. Table 1 lists the victims- and offender-related variables and their measures. The features selected are representative of all the information that could have been retrieved from victims and offenders.

3.4. Dependent variable

3.4.1. Fraud

The dependent variable was fraud. We coded fraud as 0 when no fraud was committed and 1 when fraud was committed. We used the *Canadian Criminal Code* (CCC) definition to operationalize fraud as a construct in the coding process. Section 380 (1) of the CCC defines *fraud* as an act in which

> [e]very one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretense within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service. (Justice Law, 2021)

[2] Pandas is an open-source software library written in the Python programming language for data analysis and manipulation.

Table 1
Descriptions and measures of independent variables.

Feature	Description	Measure	Indicators
Investors	Number of investors	Continuous	
Invested	Amount of money invested	Continuous	
Loss	Amount of money lost	Continuous	
Commissions	Commission earned	Continuous	
Off_exp	Offenders' experience in the industry	Continuous	
Inv_age	Investors' age	Continuous	
Inv_income	Investors' income	Continuous	
Inv_liquid_asset	Investors' liquid assets	Continuous	
Inv_networth	Investors' net worth	Continuous	
District_council	IIROC district council that heard the case	Categorical	ON, Que, AB, B.C., Atlantic, West
Occupation	Offender's occupation	Categorical	Advisor, executive, manager
Bank_owned	Bank-owned investment firm	Categorical	Bank-owned; not bank-owned
Firm_type	Type of firm	Categorical	Retail; institutional
Off_sex	Sex of offender	Categorical	Male; female
Discip_hist	Disciplinary history of offender	Categorical	History; no-history
Inv_sex	Sex of investor	Categorical	Male; female
Inv_emp	Employment status of investor	Categorical	Employed; unemployed
Inv_retired	Retirement status	Categorical	Retired; not retired
Knowledge	Knowledge level of investor	Categorical	Poor, average, good
Relationship	Investor's relationship to offender	Categorical	Acquaintance; family

3.5. Machine learning model strategy

We performed the analysis using the Python programming language. Python is an open-source, general-purpose programming language that uses Scikit-learn, which is a free software library built to work with the Python programming language. Its functionality includes various regression and classification algorithms, clustering, preprocessing, and model selection. The evaluation of classification algorithms in Python is based on the accuracy score. However, because fraud detection is based on a classification model (i.e., fraud or non-fraud), the performance metrics also include the criteria in the classification report (precision, sensitivity, and precision). Because of imbalanced data sets, the measures in the classification report are more reliable than the accuracy score (Cook & Ramadas, 2020). The receiver operating characteristic (ROC) curve is another metric used to evaluate the classification performance of different algorithms. The ROC plot is a trade-off between the false positive and the true positive in the confusion matrix. The closer the ROC curve is to 1, the more efficient the model performance is.

3.6. Data cleaning

General unstructured data can be exceptionally messy—"garbage in, garbage out". The model can only be accurately constructed based on the source data. If the data are not cleaned for duplicates and inaccurate observations, there is a strong chance that the model will be misrepresented along with the relationship between the features and target variables. The algorithm learns based on the data fed into it, and those data represent real-world transactions. In this study, it was particularly important that we cleaned the feature variables used to predict fraud so that they accurately represented the hypothesized relationship between the featured observations and the general data. One should consider how costly it would be if the model were inaccurate in fraud detection or elicited a significant number of false positives (i.e., type 1 errors). In other words, messy data can lead to the "garbage in, garbage out" effect and, therefore, lead to unreliable outcomes. Because of this important fact, the first step in the data preprocessing is to clean up messy and unstructured data.

3.7. Encoding categorical data

As aforementioned, a significant proportion of the feature variables were nonnumerical (i.e., categorical), and we had to encode them using one-hot encoding (ONE) and label them using Scikit-learn. ONE is a program that transforms categorical variables based on the number of unique values in the feature. One example is the nominal value "occupation", which represents the occupation of the offender and takes the strings "advisor", "manager", and "executive" to represent the three categories. Machine learning models cannot interpret such string values, so we preprocessed them into a numerical format to separate features—namely, with categories such as "advisors", "managers", and "executives". One of the problems with ONE arises from categorical features with high cardinality (or too many values). Categorical features with many values generate far too many columns. In this data set, the only feature with more than three columns was "district council", which we categorized into six columns representing the four largest Canadian provinces (Ontario, British Columbia (B.C.), Alberta, and Quebec); the other two columns represented the smaller Atlantic and Western provinces.

3.8. Treating duplicate and missing values

Some numerical columns also had duplicate values, which we dropped from the data set. Additionally, various columns had missing values. In the columns representing numerical features, the value "NA" represented an actual missing value. To account for missing values, we inferred from the univariate analysis and imputed the mean, median, and mode. For variables with large outliers, we used the median value to replace empty cells, and for variables with a normal distribution, we used the mean to impute for missing values. For example, the feature "invested", representing the amount investors had spent, had rows of missing values. The univariate analysis indicates that this feature was right-skewed. As such, using the mean would have presented a feature biased toward the far right of the distribution. In such cases, we asserted that the median represents most values for this particular feature.

3.9. Featuring engineering and variable transformation

Models based on the machine learning workflow develop from certain assumptions about the data. One of these assumptions is that the data of all features must be transformed into numerical or integer variables, which can be accomplished through feature engineering and variable transformation. Feature engineering can convert nonnumeric features into numeric features. For example, in this paper, the feature "district council" represents the following Canadian provinces with regard to the IIROC's hearing panels: Ontario, Quebec, Alberta, Nova Scotia, Manitoba, B.C., Prince Edward Island, Saskatchewan, and New Brunswick. Transforming these features into their respective categorical variables would have made for some redundant features that contributed nothing to the classification model. Although most of the cases were from Ontario, Quebec, and Alberta, we kept them as separate features. We transformed the other features (Nova Scotia, Manitoba,

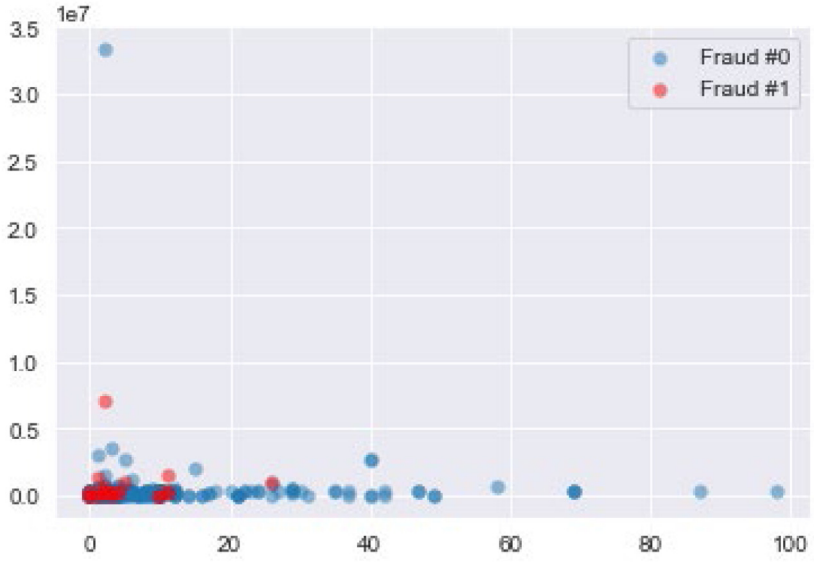

Fig. 1. Class imbalance of fraud.

PEI, Saskatchewan, and New Brunswick) into two separate categorical variables to represent the Western and Atlantic Provinces.

Scaling standardized all the numeric features so that numbers were on the same scale of units. Many numerical features in this data set did not follow a normal distribution. As such, we used scaling to normalize the data to bring the numerical features into the same range. The approach that we used to scale the numerical features was min–max scaling, which standardized all values between 0 and 1. Scaling is an important step because variables that are measured at different raw values can lead to biased models. For example, in this data set, the amount of money invested can range from $10,000 to $1,000,000, and the commission earned can range from $20,000 to $40,000. Using min–max scaling, we scaled all the values for these two variables between 0 and 1. It is likely that the minimum and maximum (or outlier) values of the numeric features could highly influence min–max scaling. However, with min–max scaling, we compressed all the outliers into a narrow range and amalgamated them to standardize the data.

3.10. Addressing class imbalance

Classification models sometimes suffer from class imbalance. While conducting the univariate analysis of this data set, a cross tabulation indicated that the dependent variable "fraud" suffered from a class imbalance in which 5% of the observations were fraud and 95% were not fraud. The risk of proceeding to build the models with a class imbalance is that either the train or test set could ultimately receive a significant number of the fraud cases. For example, the training set could be trained on most of the fraud observations, whereas the hold-out set is tested without any fraud observations. The result would be that the learning model would place more emphasis on the majority class (non-fraud) and potentially result in overfitting (Jackson, 2015). In other words, the model would have trained to such an extent on the training set that it failed to recognize the fraud observations in the classification and could have easily produced too many false negatives (Lokanan & Liu, 2021). Fig. 1 clearly shows the class imbalance. It is evident that the fraud cases are scattered throughout the data set and that there were few cases.

To address class imbalance issues, we used the synthetic minority oversampling technique (SMOTE) to reclassify the imbalance of the target variable (see Lokanan & Liu, 2021; Smiti & Soui, 2020). In particular, we performed minority oversampling (up-sampling) to increase the number of fraud observation in the data set. To up-sample the target variable, we created "synthetic elements" to add new fraud cases through linear interpolation techniques (p. 9). As Fig. 1 depicts, SMOTE effectively "focuses the decision region of the minority class" to be more general and balanced with the majority class data as well as increases fraud observations (p. 327). With SMOTE resampling, the fraud observations are more visible in the data set. Fig. 2 displays red dots moving closer to the blue dots; this movement indicates that SMOTE effectively balanced the number of fraud and nonfraud observations.

3.11. Train/test splits

To build the machine learning model, we split the data into a 70/30 train/test hold-out validation. To be more specific, the model held out 30% of the data as the test set and trained on the other 70%. We used the training set to learn the optimal parameters, given the label data. The test set is a separate set that holds out to see how well the model will perform on the unseen data. This approach ensures that the model efficiently generalizes to new situations. The train/test splits are independent of one another because there are often times where parts of the test data may ultimately leak into the training data (i.e., data leakage) and compromise the model. When data leakage occurs, the test data is no longer classified as unseen data. To evaluate the model on the test data, the algorithm first predicts the label or the numerical value of the model and compares the results with the actual value of the training model. To measure the error of the model, the error metric between *y test* and *y predict* is evaluated assuming that the model is evaluating a data set that it has never seen before. The error metric demonstrates how well the model performs on the unseen data.

4. Algorithms considered

4.1. Logistic regression

Despite its name, logistic regression is a linear model for classification rather than regression (Lokanan & Liu, 2021). The basic idea behind logistic regression is that it transforms the linear function $0 + \beta 1X$ as well as maps it in two or more discrete classes using the logistic sigmoid function $S(t)$. The probabilities are plotted as an S-shaped curve, governed by the following equation:

$$P(X) = \left(\frac{(e)^{b+b'X}}{1+(e)^{b+b'X}} \right),$$

where,

P is the probability,

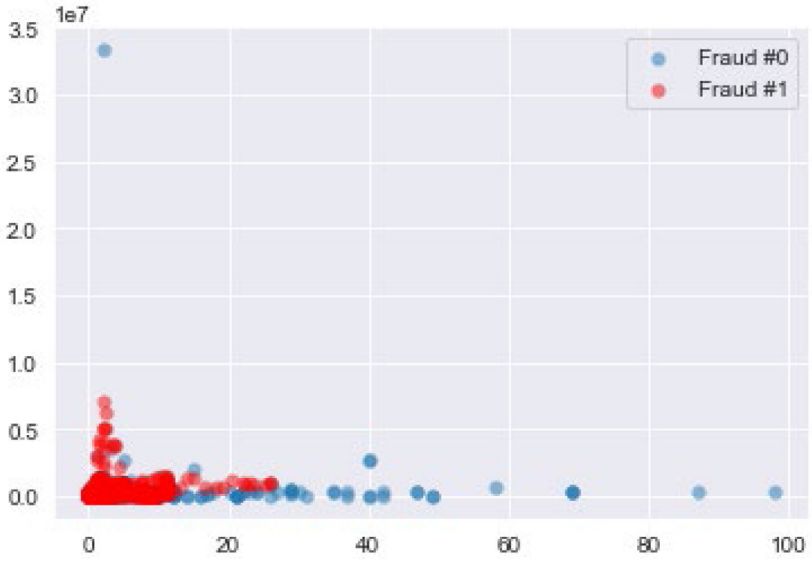

Fig. 2. SMOTE data balance.

X is the input set, and

b *and* b' are the corresponding coefficients calculated using maximum-likelihood estimation while training.

Logistic regression is one of the most popular machine learning methods used for classification purposes because it is easy to implement, easily extended to multiple classes, and efficient for classifying new records (Alenzi & Aljehane, 2020; Bala & Garg, 2019; Salillari & Prifti, 2016). For fraud detection purposes, logistic regression is unique because it can provide the ranking order of the classified data set on the probability of fraudulent versus nonfraudulent activities (Maranzato et al., 2010).

4.2. Decision Tree Classifier (DTC)

The DTC uses a tree-like graph to approach multistage decision-making and predict a final decision. The trees are generated by arranging the data set into multiple branching segments in agreement with decision rules, thus identifying the worst, best, and expected values of different scenarios (Cody et al., 2015; Gaikwad et al., 2014). Two common metrics are used to split the classification: Gini impurity and information entropy. In brief, the Gini impurity is the probability that a piece of data randomly chosen from the data set would be incorrectly labeled. Entropy works similarly. The attribute of the minimum entropy is selected to generate a decision tree node. Recursion is then used on the remaining nodes to complete the decision tree. The entropy can be defined by the following equation:

$$S = \sum_{i=1}^{C} (-p_i \log_2 p_i),$$

where,

S is the entropy,

c is the number of classes, and

p_i is the most frequent probability of class i.

The usefulness of DTC in fraud detection arises from its ability to compensate for missing values without any imputation. DTCs are easier to interpret than most other classifier models, and they can handle skewed or outlier data without any major transformation (Mitchell, 1997; Song & Lu, 2015). Because they can aggregate the results of decision trees in a model, DTCs can substantially improve fraud prediction.

4.3. Random Forests Classifier (RFC)

The RFC is an ensemble of decision-tree classifiers that builds large collections of decorrelated trees and aggregates the prediction of each tree to assign a class by majority vote (Aria et al., 2021; Bhattacharyya et al., 2011; Dietterich, 2000). As a member of the supervised learning algorithm family, this method uses a random subset of the full training set to train each tree independently from the others and then splits each node based on a feature selected from the random subset without any pruning (Altendrof et al., 2005; Azar et al., 2014; Ho, 1995). Mathematically, the final classification is expressed as the following:

$$H(x) = arg\ max\ _Y (\sum_{i=1}^{n} I(hi\,(x) = Y)),$$

where,

h_i corresponds to single-decision-tree model trees,

Y is the target output, and

I is the indicator function.

Random forest algorithms are considered applicable to fraud detection because they are more accurate and robust to noise than single-based classifiers (Breiman, 1996; Dietterich, 2000). Moreover, given an internal unbiased estimate of generalization errors, random forest algorithms are efficient for both large and small databases, resistant to overfitting, robust to outliers, flexible with the handling of different data attribute types, and computationally lighter and faster than other tree ensemble methods (Altendrof et al., 2005; Aria et al., 2021; Bhattacharyya et al., 2011; Breiman, 2001; Quinlan, 1986).

4.4. CatBoast

The CatBoast algorithm is an open-source, gradient-boosting library that builds consecutive decision trees and minimizes the loss with each tree generated (Hancock & Khoshgoftaar, 2020). CatBoast is considered a "greedy" algorithm because it solves exponential growth related to feature combinations by selecting the ones that improve the loss function (Al Daoud, 2019). The CatBoast library has gained recognition since its release in 2017 because of its wide functionality for evaluating the learning process and its large range of functions for assessing the effectiveness of training sets (Prokhorenkova et al., 2018). Moreover, CatBoost algorithms are considered more appropriate for imbalanced data and have an inbuilt feature that automatically handles categorical features (Hancock & Khoshgoftaar, 2020). The ability of CatBoast to handle large amounts of categorical data smartly and efficiently, along with its computational speed, makes it an effective algorithm for fraud prediction.

4.5. Hyperparameter tuning with GridSearchCV (GSCV)

GSCV is a function in the Scikit-learn's model selection package for the Python programming language. **The grid search that GSCV**

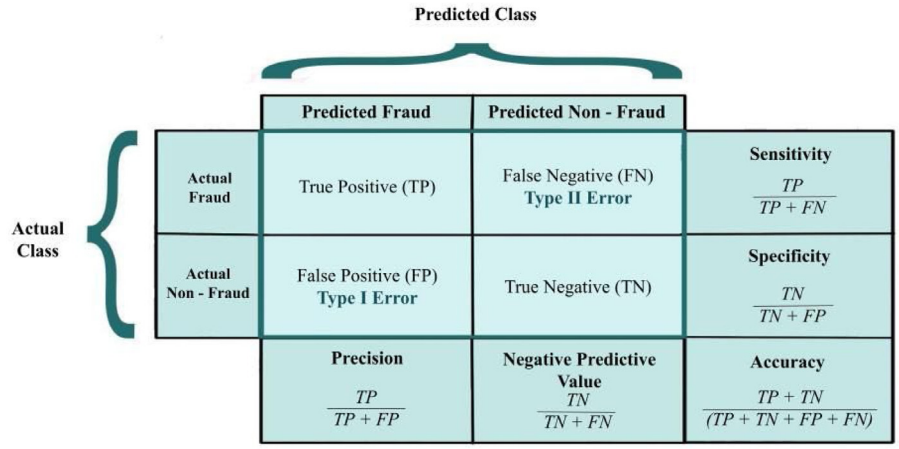

Fig. 3. Advanced classification matrix.

Table 2
Numerical features.

	Count	Mean	Std	Min	25%	50%	75%	Max
Year	405	2.01E+03	3.06E+00	2006	2010	2012	2015	2019
Investors	406	8.44E+00	1.22E+01	0	1	4	10	98
Loss	393	3.66E+05	1.75E+06	0	0	279000	365823	33345000
Invested	396	2.98E+06	8.16E+06	0	246849.3	2050808	2975602	85000000
Commissions	406	4.78E+04	6.17E+04	445	38992	38992	38992	688085
Off_exp	352	1.61E+01	8.62E+00	5	9	12	23	43
Inv_age	132	6.27E+01	1.31E+01	19	56.75	62	69	94
Inv_income	406	1.23E+04	7.87E+04	0	0	0	0	1500000
Inv_liquid_asset	406	4.46E+04	1.93E+05	0	0	0	0	2400000
Inv_networth	406	1.38E+05	1.06E+06	0	0	0	0	20000000

provides exhaustively generates a list of candidates from a specified list of parameter values to further hypertune the model. GSCV considers all possible combinations of parameter values when fitting the data set (Shuai et al., 2018; Varoquaux et al., 2015). GSCV is tremendously valuable in fraud detection research because it fits all possible combinations of parameters and chooses the best model based on accuracy with cross-validation. Thus, instead of merely using a train/test split, GSCV has inbuilt functions that run five-fold cross-validation on the test data. Individual algorithms, such as RFC or DTC, will not give perfect accuracy scores. This is highly problematic because, in fraud detection research, even a 1% or 2% difference in the accuracy can prove fatal (Rtayli & Enneya, 2020). Error in fraud detection can occur in two ways: classifying fraud cases as non-fraud and classifying non-fraud cases as fraud. Hence, GSCV helps improve the results and manages to hypertune the model to improve the accuracy of the individual algorithms.

5. Analysis of findings

5.1. Summary statistics

Table 2 presents the descriptive statistics of the numerical feature variables. The average amount invested is $2,975,602, and the average loss incurred is $360,000. Given the average loss per investor, it is not surprising that the average commission earned is $47,815. There is an outlier loss in the amount of $33,345,000; it was potentially a case in which there were multiple investors or high net worth investors. Interestingly, investors' average liquid net worth at the time of the investment was only $44,621, whereas their total net worth was $137,608. These findings indicate that the investors were not particularly wealthy either. Given that the average investor's age was 63 and they were potentially close to retirement, losses of this magnitude can have detrimental effects on their mental well-being (Boyd, 2005; Lokanan & Liu, 2021).

Table 3 presents the descriptive statistics of the categorical features. Most of the offenders were advisors from bank-owned investment firms. There also appears to be an association between male offenders (i.e., investment advisors) and female investors (see Lokanan & Liu, 2021), which may be because of a common occurrence in which investment advisors gain the trust of their female investors and then swindle them of their life savings—a point well established in the literature on fraud victimization (Lokanan, 2017; Reisig & Holtfreter, 2013; van Wyk & Mason, 2001). Most of the victims were unemployed with poor investment knowledge. These findings corroborate previous research showing that investors with poor financial knowledge are more like to be preyed upon by trusted financial advisors than those with excellent financial knowledge (Deliema et al., 2020; Drolet, 2016). As a group, female investors with poor financial knowledge are more likely to become victims of fraud than their male counterparts.

6. Performance evaluation

6.1. Accuracy

Table 4 shows the accuracy score of the classification algorithms. The four metrics we used to evaluate performance were true positive (TP), false positive (FP), true negative (TN), and false negative (FN). TP predicted 1 when the actual class bias was 1; FP predicted 1 when the actual class bias was 0; TN predicted 0 when the actual class was 0; and FN predicted 0 when the actual class was 1. The formula to calculate the accuracy score was the following:

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + FN + TN}$$

We defined the accuracy by the ratio of the total number of predicted outcomes classified as correct. As Table 3 depicts, the RFC had the highest accuracy score (98%) for hold-out sets. In fraud prediction, even a small percentage difference can prove fatal. In a situation in which there is a Type 11 error (FN), fraud is present, but the classifier incorrectly predicts that there is no fraud. In fraud prediction, incorrect

Table 3
Categorical features.

	District_council	Occupation	Bank_owned	Firm_type	Off_sex	Discip_hist	Inv_sex	Inv_Emp	Inv_Retired	Knowledge	Relationship	Fraud
Count	406	403	389	392	405	326	406	397	394	68	43	406
Unique	9	3	2	2	2	2	2	2	2	3	2	2
Top	Ontario	Advisor	No	Retail	Male	No	Female	Unemployed	No	Poor	Acquaintance	No
Freq	165	316	256	390	361	290	346	364	362	38	36	385

Table 4
Accuracy score of classification algorithms.

	Accuracy score	
Model type	Training score	Testing score
Logistic regression	.85	.84
DTC	.83	.75
RFC	.1	.98
CatBoast	.98	.95
GridSearch	.1	.99.5

Table 5
Classification techniques scores.

Techniques	Sensitivity/recall	Specificity	Precision	F-measure
Logistic regression	0.90	0.80	0.80	0.84
DTC	0.91	0.90	0.7	0.79
RFC	0.98	0.90	0.99	0.99
CatBoast	0.95	0.90	0.97	0.96
GridSearch	0.1	0.90	0.99	0.1

classifications are significant because the classification that predicts a fraudulent transaction as non-fraudulent can cause significant losses for investors (Hooda et al., 2018; Perols, 2011; Perols et al., 2017). Given that the average loss per investor is $360,000, reducing the FP (i.e., Type 1) error is a significant challenge. FP results have proven problematic in fraud detection. It is important for the algorithm to have high accuracy to reduce the false positive score. To improve the model, we employed GSCV to optimize the performance in the accuracy score. With GSCV, the accuracy score for the test set increased to 99.5%, thereby reducing the number of FP predictions to near zero. In addition, the DTC score is lower than all the other scores—perhaps because the features are independent of each other and because the DTC partitions the feature space into rectangular regions that are then modeled on the mean responses of the data points (Cody et al., 2015; Song & Lu, 2015).

6.2. Classification matrix

With imbalanced data sets, the accuracy score, although an important performance metric, can be misleading and should be used in tandem with another metric. The main problem with using raw accuracy to measure the efficiency of a model is that it only accounts for the true positives/negatives and not the false positives/negatives of the model (Johnson & Khoshgoftaar, 2020; Qian et al., 2020). A good, user-friendly metric that can be used alongside accuracy is the classification report. The classification report is a more advanced metric based on the confusion matrix, expressed in Fig. 3. The model shows the confusion matrix of two classes: predicted fraud and predicted non-fraud.

Based on the mathematical formula in Fig. 3, the advanced classification report scores are shown in Table 5. Of the individual algorithms, the RFC has the highest sensitivity score (.98). The sensitivity metric, as aforementioned, measures the true positive rate (TPR), or all the observations that the classifier labels as positive. The sensitivity metric is intended to help researchers recall (or measure) the percentage of fraudulent observations (i.e., the positive class) that the algorithm correctly predicts. In this study, the RFC outperformed the other individual algorithms—98% of the observations that it labeled as fraud were, in fact, fraudulent observations. This percentage is called the capture rate and shows the proportion of fraud cases that the model correctly captures or predicts.

With the exception of logistic regression, the specificity, or the TPR, was relatively high for all the techniques, at 90%. The specificity metric measures how correctly the model predicts actual negative classes. In other words, if the model identifies all the negatives correctly, the false positive rate (FPR) is zero. By this logic, every non-fraud observation predicted incorrectly as fraud will increase the FPR of the model. In this study, we specifically examined how often the models correctly identified observations that were not fraud. The models are consistent in that the proportions of observations classified as non-fraud were actual non-fraud observations.

Another important metric is precision. The precision ratio measures the number of classified positive classes that the algorithms correctly predicted as positive. The precision rate of the positive predicted value is a conditional probability that the true class is 1 if the predicted class is 1 (Lever et al., 2016). In this study, the following question guided the precision rate: when the model predicts fraud, how often is it correct? As Table 5 reveals, the RFC (99%) and GSCV (99%) techniques had the highest precision ratio, meaning that 99% of the observations classified as fraud were indeed fraud. Precision is highly important in fraud classification problems (Almhaithawi et al., 2020; Bhatia et al., 2016; Campus, 2018; Hooda et al., 2018). If one were examining all observations related to fraud, the actual class is whether the observations are about fraud or not. The TP would indicate that the algorithm correctly identified all observations that were fraud. The FP in this case meant that some observations were flagged but were non-fraud. This is where precision would be useful because it would measure the percentage of observations that were fraud.

The F-Measure is the harmonious mean of sensitivity and precision. The F-Measures capture the trade-offs between precision and sensitivity. As shown in Table 5, the RFC and GSCV have the highest sensitivity and precision scores, respectively. In this situation, the F-measure can be used to compute and balance out the sensitivity and precision scores into metrics for both the RFC and GSCV. A closer look at Table 3 shows that the F-score was 99% for RFC and 100% for GSCV. For all observations that were not fraud, the model predicted 99% (as in the RFC model) and 100% (as in the GSCV model). These findings indicate that the F-measure effectively balanced out the consistency of the specificity scores for all the techniques with precision scores. In this particular case, there was a combination of high sensitivity and high precision for GSCV, indicating that the model handled the fraud and non-fraud classification effectively.

6.3. Area under receiver operating characteristic curve (AUROC)

In Fig. 3, the main problem with using accuracy as a performance measure is that it only accounts for the TP and TN negative observations and ignores the FP and FN observation (Almhaithawi et al., 2020; Cody et al., 2015; Cook & Ramadas, 2020). Thus, in effect, the accuracy matrix does not account for the Type 1 and Type II errors. A better measure would be needed—one that would take into consideration all performance information as a single score while also accounting for imbalanced data sets. The AUROC is a more reliable metric because it plots the trade-off between the FP rate and the TP rate (i.e., precision) for different choices among binary classification models (Lever et al., 2016). The AUROC is a measure of the usefulness of the test. The greater the area under the curve (AUC), the more useful the test; the AUC is mapped between values of 0.5 and 1 (Cook & Ramadas, 2020). Comparative AUROC scores for the individual algorithms and the GSCV

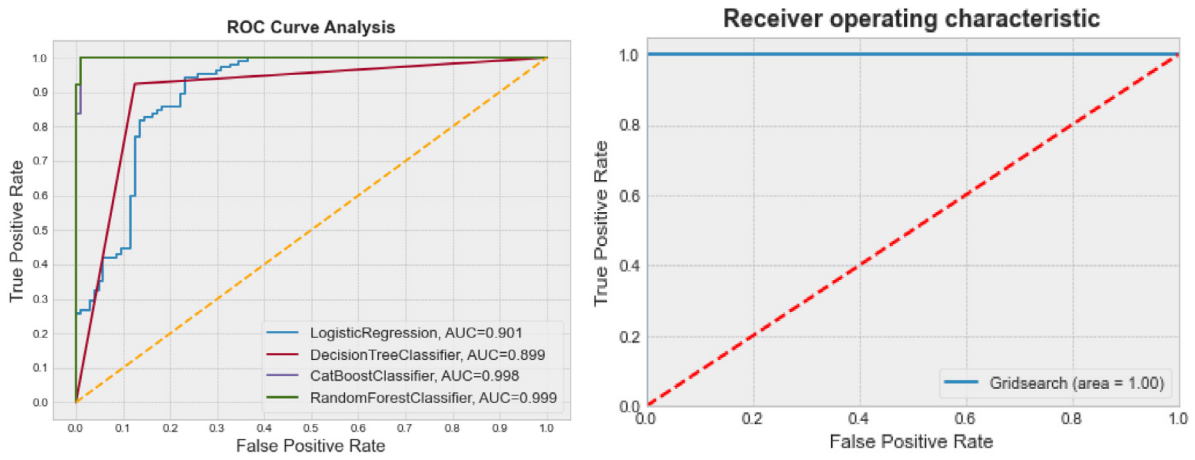

Fig. 4. Side-by-side ROC individual algorithm and GridSearch ROC plots.

appear in Fig. 4. Of the individual algorithms, the RFC performed better than the other three models, whereas the GSCV model was slightly better than the RFC with a score of 1.00. These findings indicate that both the RFC and GSCV models were effective in predicting fraud because the TPR and FPR were closer to 1 in both the RFC and GSCV models. Additionally, the RFC and GSCV's AUC corresponded with the high precision scores for these two techniques, as shown in Table 3. The TPR was superior to the FPR for both models.

6.4. Feature importance

Fig. 5 presents the variable importance estimates for the RFC model. Feature importance shows the relative contribution of each predictor variable to the dependent variable, which is fraud. Across all features, the amount of money invested and whether the offender was from a bank-owned investment firm were the high predictors of fraud in terms of the standardized coefficient. These findings have corroborated previous research, indicating that regulators cast their nets for smaller investment firms at the expense of the larger bank-owned firms to give the impression that they are regulating in the public interest (see Fair Canada (2014) and Lokanan (2015). The money loss from the investment, the register representative's registration with the B.C. district council, and the number of investors per case complete the top five features because of their importance in modeling fraud prediction.

Compliance deficiencies are not surprising in B.C. A recent inquiry by the British Columbia Securities Commission found that more investment advisors are in noncompliance with securities regulations in B.C. than in other provinces (Manchester, 2021). These findings do not suggest that registrants who are registered in the B.C. district council will inevitably commit fraud but that branch managers under B.C. jurisdiction and regulators should scrutinize portfolios with significant investments for signs of fraud. Branch managers, in particular, should pay careful attention to portfolios that are incurring losses periodically because such is a sign of potential fraud. If the client invested a significant amount, is incurring losses, is from a bank-owned firm, and is registered with the B.C. district council, then the branch manager should closely monitor the registrant responsible for that account. Financial advisors with a large client base should also be scrutinized by their branch managers to ensure that they comply with their clients' investment objectives, purpose, and risk tolerance.

Even though the DTC performed poorly relative to the other classification models, the tree plot in Fig. 6 is significant because it split the population into two sub-population base on the most important feature. Fig. 5 reveals that the amount of money invested was the top feature predictive of fraud. This classification repeats itself in the decision tree model in Fig. 6. As Fig. 6 depicts, the DTC distinguished the amount of money invested from the other features as the root node. Of all the features used in the model, the DTC determined that the best way to split the fraud and non-fraud class was by the amount of money invested. If the value of the amount invested was less than 0.5 for an observation, then it was 0 (non-fraud) or placed under the "True" branch. In cases where the value of the observation was greater than 0.5, then it was placed in the "False" (or fraud) branch in the tree plot. In this case, the key player was the district council of B.C., which incidentally is among the top five features to predict fraud (see Fig. 4).

7. Discussion

In this paper, we employed an exploratory machine learning approach to predict investment fraud in Canada. Previous researchers have most recently employed machine learning on credit card and financial statement frauds with good but inconsistent results (Cecchini et al., 2010; Fernández Delgado et al., 2014; Hajek & Henriques, 2017; Lokanan et al., 2019; Perols et al., 2017; Phua et al., 2010). We may partially attribute these inconsistencies to the techniques such researchers used, which may have introduced multicollinearity into the models, resulting in inconsistent performance.

We trained the models used in this study on 11 years of enforcement data from the IIROC's tribunal hearings. Furthermore, we used four algorithms in the models: logistic regression, DTC, RFC, and CatBoast. We used the GSCV to further fine-tune the RFC for optimal results. The results have indicated that advanced machine learning algorithms can be used by analysts to accurately predict fraud in financial markets. Given the data and the performance metrics used in this paper, the main conclusion is that the RFC, when further tuned using the GSCV, can generate more accurate results compared with the results from logistic regression, DTC, and the CatBoast algorithms. Of the individual algorithms, the RFC accounted for 99% accuracy (testing) and, when further fine-tuned with the GSCV, performed slightly better with 99.5% accuracy in predicting fraud.

This study has presented a novel approach for regulators to predict fraud in financial markets using machine learning techniques. These techniques offer several advantages over traditional statistical techniques of fraud detection (see Wall, 2018). In doing so, the study has contributed to the extant literature on the link between SROs and market regulation and, at the time of writing, presents the first machine learning model to use conventional victims, offenders, and enforcement features to predict fraud in financial markets. Specifically, although previous researchers have employed machine learning techniques to predict fraud and fraud victimization in different domains using financial and demographic variables (Cecchini et al., 2010; Lokanan & Liu, 2021; Perols et al., 2017) *this study is the first whose authors have examined symptoms of fraud and explored specific variables pertaining to SROs' regulation of the financial markets.*

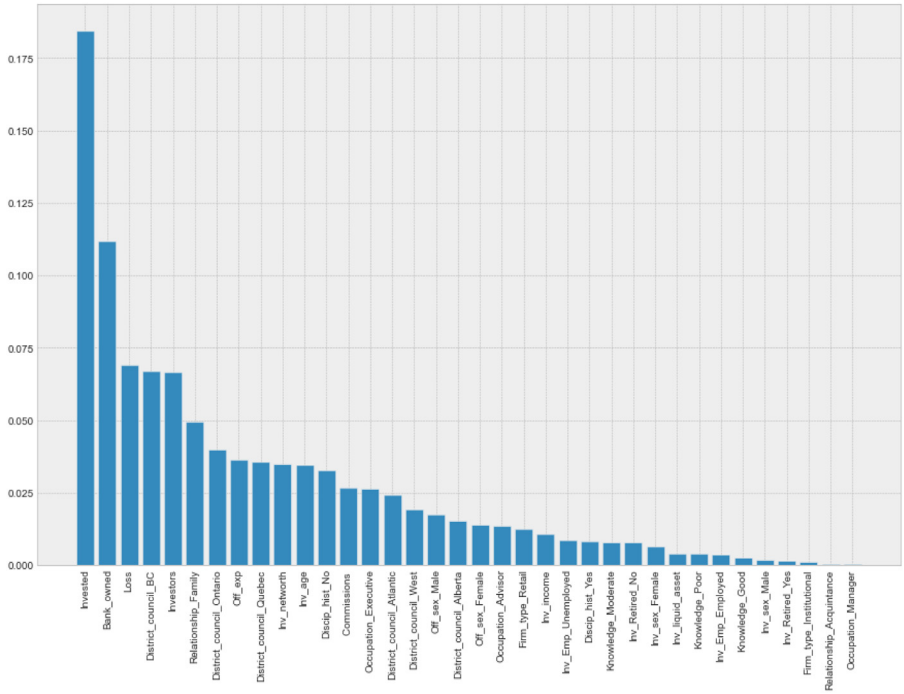

Fig. 5. Feature importance in fraud prediction.

.

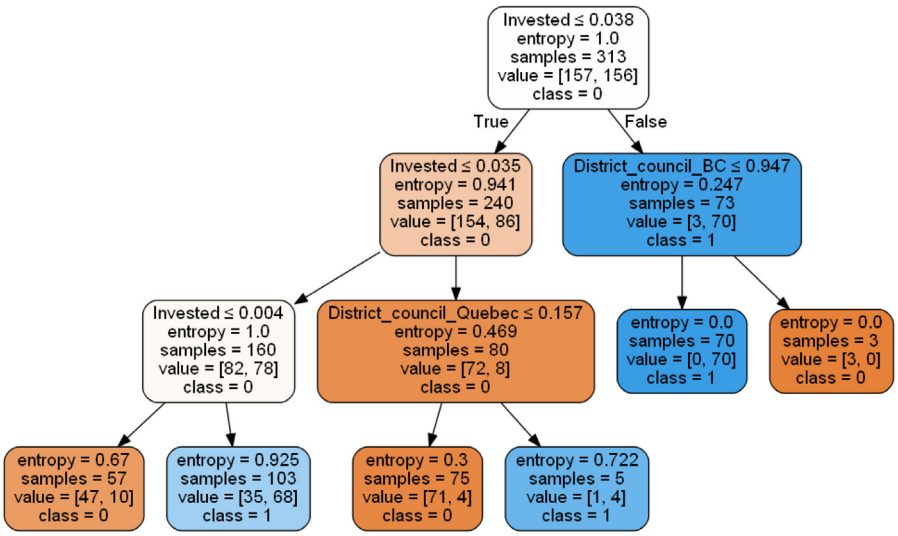

Fig. 6. Decision tree plots.

Self-regulation has been the prevailing regulatory method for market surveillance in Canada. Although self-regulation has been criticized by scholars for not regulating in the public interest (Lokanan, 2017; Paton, 2007; Williams, 2012), machine learning for fraud detection offers some space to mitigate these criticisms. The use of machine learning algorithms to detect fraud could provide many benefits for regulators and market participants. At the regulatory level, machine learning algorithms could allow regulators to be proactive and identify red flags at an early stage in the compliance process (Cohen, 2012; Kuhlmann & Saks, 2008; Soliman et al., 2011); at the firm level, managers could use machine learning to minimize Type 1 errors in the hiring process (Hildebrandt, 2018); and, at the retail investor level, the use of machine learning technology could play an important role in fraud awareness (Lokanan & Liu, 2021). Taken together, the use of computational technology offers regulators and other stakeholders unique opportunities to improve market surveillance to detect fraudulent conducts before they occur (Narang, 2021; Soliman et al., 2011).

For self-regulatory regimes to ward off government intervention, they must modernize enforcement through computational technology (Lokanan & Liu, 2021; Soliman et al., 2011). Such regimes must perceive computational technology as an essential tool for identifying hot spots of fraud in real time (Braithwaite, 2013; Lokanan, 2018). They could use machine learning techniques to identify features and provide analysts with real-time threshold scores to prevent fraud as well as examine features such as the amount invested, the number of clients managed, their relationship to the registrants, and, more generally, rogue trading in the marketplace (Narang, 2021; Williams, 2012; Yeung, 2018). Machine learning techniques offer opportunities for customized outcomes while improving surveillance and compliance not only for individual registrants but also at the firm level (Hildebrandt, 2018; Shiell & Chapman, 2000). One way to improve the prevention of market abuse in trading is to use machine learning to automate systems that monitor a variety of behaviors by investment advisors (Wall, 2018). Such behaviors involve the type of client, the

number of clients, the amount of money involved, and even the amount of planning and organization that goes into the advising process (van Liebergen, 2017). Machine learning techniques could provide valuable input to industry self-regulation and move regulatory technology closer to helping SROs improve their general fraud detection and prevention programs.

8. Conclusion

Many challenges are inherent in the successful implementation of machine learning techniques in financial market regulation. Chief among these is the fact that machine learning prediction is less transparent than traditional models based on hypothesis testing and statistical inferences. The process by which machine learning models reach predictions is unclear. Machine learning models provide prediction scores, but the process by which these scores are determined is not yet well established in the literature. Unlike the statistical approach, machine learning is focused on the prediction base in performance metrics. Consequently, machine learning predictions could identify relationships that have not been established in the literature. For example, a premise based on the relationship between two variables in which there is no evidence of causality could be exploited, hence suffering from interpretation bias.

Despite these limitations, machine learning techniques offer promising opportunities for the prevention and mitigation of fraud in financial markets. In this study, we took an iterative approach by consistently applying four established machine algorithms to identify a relationship between selected features and fraud that would probably not be detected with a human-centered approach to market surveillance. These machine learning techniques offer SROs the tools to identify potential fraud, putting them in a better position to anticipate the impact of regulatory changes on the modernization of enforcement in Canada.

Future researchers must consider the application of machine learning techniques to improve fraud detection in financial markets. Although regulatory agencies have implemented policies to better censure fraud, they will also need to deploy more innovative technology to develop advanced solutions. One way is to develop testable hypotheses on propositions from theories of crime to identify the features of the typical fraudster in financial markets. An ideal way to start this interdisciplinary inquiry is to develop research questions on machine learning techniques that will aid in recognizing criminal motivation to circumvent laws guiding fair practices. The study of fraud in financial markets needs as many proposals as possible—with the hope that one will break through and provide new insights on regulatory technology for fraud detection and prevention.

CRediT authorship contribution statement

Mark Eshwar Lokanan: Writing – review & editing, Methodology, Supervision. **Kush Sharma:** Data coding, Literature Review.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The Social Sciences and Humanities Research Council of Canada Grant number: 200681.

References

Al Daoud, E. (2019). Comparison between XGBoost, LightGBM and CatBoost using a home credit dataset. *International Journal of Computer and Information Engineering*, *13*(1), 6–10.

Alini, E. (2020). 90-Year-old RBC client allegedly lost $60k to fraud by longtime advisor. In *Global news. newspaper article from november 19*. Retrieved 23 April, 2021 https://globalnews.ca/news/7465223/90-year-old-rbc-client-60k-fraud-advisor/.

Almhaithawi, D., Jafar, A., & Aljnidi, M. (2020). Example-dependent cost-sensitive credit cards fraud detection using SMOTE and Bayes minimum risk. *SN Applied Sciences*, *2*(9), 1–12. http://dx.doi.org/10.1007/s42452-020-03375-w.

Altendrof, J., Brende, P., & Lessard, L. (2005). Fraud detection for online retail using random forests. Technical Report. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.143.71&rep=rep1&type=pdf.

Aria, M., Cuccurullo, C., & Gnasso, A. (2021). A comparison among interpretative proposals for random forests. *Machine Learning with Applications*, http://dx.doi.org/10.1016/j.mlwa.2021.100094.

Azar, A. T., Elshazly, H. I., Hassanien, A. E., & Elkorany, A. M. (2014). A random forest classifier for lymph diseases. *Computer Methods and Programs in Biomedicine*, *113*(2), 465–473.

Baggot, R. (1989). Regulatory reform in Britain: The changing face of self-regulation. *Public Administration*, *67*(4), 435–454.

Beneish, M. (1999). Incentives and penalties related to earnings overstatements that violate GAAP. *The Accounting Review*, *74*(4), 425–457.

Bhatia, S., Bajaj, R., & Hazari, S. (2016). Analysis of credit card fraud detection techniques. *International Journal of Science and Research*, *5*(3), 1302–1307.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602.

Boyd, N. (2005). Eron mortgage study. In *British columbia securities commission*. https://www.bcsc.bc.ca/-/media/PWS/Resources/News/News_Releases/Eron_Research_Study.pdf.

Braithwaite, J. (2013). Flipping markets to virtue with qui tam and restorative justice. *Accounting, Organization, and Society*, *vol. 38*(6), 458–468.

Braithwaite, J., & Fisse, B. (1987). Accountability and the social control of corporate crime: Making the buck stop. *Australian Journal of Forensic Sciences*, *vol. 20*(1), 166–177.

Breiman, L. (1996). Bagging predictors. *Machine Learning*, *24*(2), 123–140.

Breiman, L. (2001). Random forests. *Machine Learning*, *45*(1), 5–32. http://dx.doi.org/10.1023/A:1010933404324.

Brockman, J. (2004). An update on self-regulation in the legal profession (1989–2000). In *Funnel in and funnel out. can. jl & soc, Vol. 19* (p. 55).

Campus, K. (2018). Credit card fraud detection using machine learning models and collating machine learning models. *International Journal of Pure and Applied Mathematics*, *118*(20), 825–838.

Canadian Securities Administrators (2020). Collaborating to protect investors and enforce securities law: FY2019/20 enforcement report. http://www.csasanctions.ca/assets/pdf/CSA-Enforcement-Report-English.pdf.

Cecchini, M., Aytug, H., Koehler, G. J., & Pathak, P. (2010). Detecting management fraud in public companies. *Management Science*, *56*(7), 1146–1160.

Cody, C., Ford, V., & Siraj, A. (2015). Decision tree learning for fraud detection in consumer energy consumption. In *2015 IEEE 14th international conference on machine learning and applications* (pp. 1175–1179). http://dx.doi.org/10.1109/ICMLA.2015.80.

Cohen, J. E. (2012). *Configuring the networked self: law, code, and the play of everyday practice*. Yale University Press.

Cook, J., & Ramadas, V. (2020). When to consult precision–recall curves. *The Stata Journal*, *20*(1), 131–148. http://dx.doi.org/10.1177/1536867X20909693.

Deliema, M., Shadel, D., & Pak, K. (2020). Profiling victims of investment fraud: Mindsets and risky behaviors. *Journal of Consumer Research*, *46*(5), 904–914.

Devlin, R., & Cheng, A. (2010). Re-calibrating, re-visioning and re-thinking self-regulation in Canada. *International Journal of the Legal Profession*, *vol. 17*, 233–281. http://dx.doi.org/10.1080/09695958.2011.580562.

Dietterich, T. G. (2000). Ensemble methods in machine learning. In *International workshop on multiple classifier systems* (pp. 1–15). Berlin, Heidelberg: Springer.

Dixon-Woods, M., Yeung, K., & Bosk, C. L. (2011). Why is U.K. medicine no longer a self-regulating profession? The role of scandals involving bad apple doctors. *Social Science & Medicine*, *73*(10), 1452–1459. http://dx.doi.org/10.1016/j.socscimed.2011.08.031.

Drolet, M. (2016). Insights on Canadian society—Gender differences in the financial knowledge of Canadians. In *Statistics canada*. ON, Canada: Toronto.

Duman, E., & Ozcelik, M. H. (2011). Detecting credit card fraud by genetic algorithm and scatter search. *Expert Systems with Applications*, *38*(10), 13057–13063.

Emeseh, E., Ako, R., Okonmah, P., O, & Ogechukwu, L. (2010). Corporations, CSR and self regulation: What lessons from the global financial crisis? *German Law Journal*, *11*(2), 230–259. http://dx.doi.org/10.1017/S2071832200018502.

Fair Canada (2014). A Canadian strategy to combat investment fraud. http://faircanada.ca/wp-content/uploads/2014/08/FINAL-A-Canadian-Strategy-to-Combat-Investment-Fraud-August-2014-0810.pdf.

Fernández Delgado, M., Cernadas García, E., Barro Ameneiro, S., & Amorim, D. G. (2014). Do we need hundreds of classifiers to solve real world classification problems?. *Journal of Machine Learning Research*, *15*, 3133–3181.

Garvie, D. (1999). Self-regulation of pollution – the role of market structure and consumer information. *Organized Interests and Self-Regulation: An Economic Approach*, *20*, 6–235, http://hdl.handle.net/10419/154822.

Gray, J., & McFarland, J. (2013). Crime without punishment: Canada's investment fraud problem. In *Newspaper article from August 24, The globe and mail*. Retrieved 18th 2020 https://www.theglobeandmail.com/report-on-business/crime-and-no-punishment-canadas-investment-fraud-problem/article13938792/.

Hajek, P., & Henriques, R. (2017). Mining corporate annual reports for intelligent detection of financial statement fraud – a comparative study of machine learning methods. *Knowledge-Based Systems*, *128*(15), 139–152.

Hancock, J. T., & Khoshgoftaar, T. M. (2020). Survey on categorical data for neural networks. *Journal of Big Data*, *7*(1), 1–41.

Heath, J. (2018). But everyone else is doing it: Competition and business self-regulation. *Journal of Social Philosophy*, *49*(4), 516–535.

Hildebrandt, M. (2018). Law as computation in the era of artificial legal intelligence: Speaking law to the power of statistics. *University of Toronto Law Journal*, *vol. 68*, 12–35. http://dx.doi.org/10.3138/utlj.2017-0044.

Ho, T. K. (1995). Random decision forests. In *Proceedings of 3rd international conference on document analysis and recognition (Vol. 1)* (pp. 278–282). IEEE.

Hoggett, E., Dubois, S., O'Connor, S., & Jamieson, R. (2019). Machine learning and the audit: Rise of the machines? KPMG. https://home.kpmg/au/en/home/insights/2019/04/audit-technology-machine-learning.html.

Hooda, N., Bawa, S., & Rana, P. (2018). Fraudulent firm classification: A case study of an external audit. *Applied Artificial Intelligence*, *32*(1), 48–64. http://dx.doi.org/10.1080/08839514.2018.1451032.

Jackson, S. (2015). The vexing problem of defining financial exploitation. *Journal of Financial Crime*, *22*, 63–78.

Johnson, J. M., & Khoshgoftaar, T. M. (2020). The effects of data sampling with deep learning and highly imbalanced big data. *Information Systems Frontiers*, *22*(5), 1113–1131.

Justice Law (2021). Criminal code (R.S.C. 1985, c. C-46). https://laws-lois.justice.gc.ca/eng/acts/c-46/section380.html.

Kaminski, K. A., & Guan, L. (2004). Can financial ratios detect fraudulent financial reporting? *Managerial Auditing Journal*, *19*(1), 15–28. http://dx.doi.org/10.1108/02686900410509802.

Klassen, R. D., & Whybark, D. C. (1999). The impact of environmental technologies on manufacturing performance. *Academy of Management Journal*, *42*(6), 599–615.

Knight, D. (2020). 2 men charged in multi-million dollar investment fraud: Lethbridge police. In *Newspaper article from july 30, Global news*. https://globalnews.ca/news/7236631/calgary-okotoks-charges-multi-million-dollar-investment-fraud/.

Kuhlmann, E., Allsop, J., & Saks, M. (2009). Professional governance and public control: A comparison of healthcare in the United Kingdom and Germany. *Current Sociology*, *57*(4), 511–528. http://dx.doi.org/10.1177/0011392109104352.

Kuhlmann, E., & Saks, M. (2008). Changing patterns of health professional governance. In *Rethinking professional governance: international directions in healthcare* (pp. 1–14). Policy Press.

Lever, J., Krzywinski, M., & Altman, N. (2016). Classification evaluation. *Nature Methods*, *13*, 603–604. http://dx.doi.org/10.1038/nmeth.3945.

Linhart, J. (2017). Can industry-wide self-regulation in the UK banking sector succeed? A law and economics perspective. *The King's Student Law Review*, *8*(1), 127–141.

Lokanan, M. E. (2015). Self-regulation in the Canadian securities industry: Funnel in, funnel out, or funnel away? *International Journal of Law, Crime and Justice*, *43*(4), 456–480.

Lokanan, M. E. (2017). Self-regulation and compliance enforcement practices by the investment dealers association in Canada: 1984 to 2008. *Journal of Financial Regulation and Compliance*, *25*(1), 2–21.

Lokanan, M. E. (2018). Theorizing financial crimes as moral actions. *European Accounting Review*, *27*(5), 901–938. http://dx.doi.org/10.1080/09638180.2017.1417144.

Lokanan, M. E. (2019). An update on self-regulation in the Canadian securities industry (2009–2016): Funnel in, funnel out, and funnel away. *Journal of Financial Regulation and Compliance*, *27*(3), 324–344. http://dx.doi.org/10.1108/JFRC-05-2018-0075.

Lokanan, M. E., & Liu, S. (2021). Predicting fraud victimization using classical machine learning. *Entropy*, *23*(3), 300. http://dx.doi.org/10.3390/e23030300.

Lokanan, M., Tran, V., & Vuong, H. N. (2019). Detecting anomalies in financial statements using machine learning algorithm: The case of Vietnamese listed firms. *Asian Journal of Accounting Research*, *4*(2), 181–201. http://dx.doi.org/10.1108/AJAR-09-2018-0032.

Manchester, J. (2021). BC securities commission finds compliance deficiencies on the rise. Retrieved May 18, 2021 https://www.castanet.net/news/Business/326242/BC-Securities-Commission-finds-compliance-deficiencies-on-the-rise.

Maranzato, R., Pereira, A., do Lago, A. P., & Neubert, M. (2010, March). Fraud detection in reputation systems in e-markets using logistic regression. In *Proceedings of the 2010 ACM symposium on applied computing* (pp. 1454-1455).

Mitchell, T. M. (1997). Artificial neural networks. *Machine Learning*, *45*, 81–127.

Narang, S. (2021). Fostering innovation and competitiveness with fintech, regtech, and suptech. In *Accelerating financial innovation through regtech* (pp. 61–79). IGI Global.: http://dx.doi.org/10.4018/978-1-7998-4390-0.ch004.

Osegi, A., & Jumbo, E. (2021). Comparative analysis of credit card fraud detection in simulated annealing trained artificial neural network and hierarchical temporal memory. *Machine Learning with Applications*, http://dx.doi.org/10.1016/j.mlwa.2021.100080.

Pai, P.-F., Hsu, M.-F., & Wang, M.-C. (2011). A support vector machine-based model for detecting top management fraud. *Knowledge-Based Systems*, *24*(2), 314–321. http://dx.doi.org/10.1016/j.knosys.2010.10.003.

Paton, P. D. (2008). Between a rock and a hard place: the future of self-regulation-Canada between the United States and the english/Australian experience. In *J. Prof. Law. Symp. Issues*. (p. 87).

Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing: A Journal of Practice & Theory*, *30*(2), 19–50.

Perols, J. L., Bowen, R. M., Zimmermann, C., & Samba, B. (2017). Finding needles in a haystack: Using data analytics to improve fraud prediction. *The Accounting Review*, *92*(2), 221–245.

Phua, C., Lee, V., Smith-Miles, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. (pp. 1–14). https://arxiv.org/ftp/arxiv/papers/1009/1009.6119.pdf.

Prokhorenkova, L., Gusev, G., Vorobev, A., Dorogush, A. V., & Gulin, A. (2018). CatBoost: Unbiased boosting with categorical features. In *Advances in neural information processing systems, 31* (pp. 6637–6647).

Qian, S. S., Refsnider, J. M., Moore, J. A., Kramer, G. R., & Streby, H. M. (2020). All tests are imperfect: Accounting for false positives and false negatives using Bayesian statistics. *Heliyon*, *6*(3), http://dx.doi.org/10.1016/j.heliyon.2020.e03571, 1-6.

Quinlan, J. R. (1986). Induction of decision trees. *Machine Learning*, *1*(1), 81–106.

Rees, V. (2013). *Transforming regulation and governance in the public interest*. Council of the Nova Scotia Barristers' Society, https://iclr.net/wp-content/uploads/2016/03/2013-10-30transformingregulation.pdf.

Reisig, M. D., & Holtfreter, K. (2013). Shopping fraud victimization among the elderly. *Journal of Financial Crime*, *20*, 324–337.

Robertson, G., & Cardoso, T. (2017). Easy money: how fraudsters can make millions off Canadian investors, get barely punished and do it again. In *Newspaper article from december 16, The globe and mail*. Retrieved 17th 2021 https://www.theglobeandmail.com/news/investigations/easy-money-canadian-securities-fraud/article37350705/.

Rtayli, N., & Enneya, N. (2020). Selection features and support vector machine for credit card risk identification. *Procedia Manufacturing*, *46*, 941–948.

Sahin, Y., & Duman, E. (2011). Detecting credit card fraud by ANN and logistic regression. In *2011 international symposium on innovations in intelligent systems and applications* (pp. 315–319).

Salillari, D., & Prifti, L. (2016). A multinomial logistic regression model for text in Albanian language. *Journal of Advances in Mathematics*, *12*(7), 6407–6411.

Severina, M., & Peng, Y. (2021). Machine learning algorithms for fraud prediction in property insurance: Empirical evidence using real-world microdata. *Machine Learning with Applications*, *5*(15), http://dx.doi.org/10.1016/j.mlwa.2021.100074.

Shiell, A., & Chapman, S. (2000). The inertia of self-regulation: A game-theoretic approach to reducing passive smoking in restaurants. *Social Science & Medicine*, *51*(7), 1111–1119. http://dx.doi.org/10.1016/S0277-9536(00)00018-6.

Sinclair, D. (1997). Self-regulation versus command and control? Beyond false dichotomies. *Law & Policy*, *19*(4), 529–559.

Soliman, W., Duchesne, R., Hall, W., Kennedy, M., & Tripp, C. (2011). Detecting credit card fraud by ANN and logistic regression. In *2011 international symposium on innovations in intelligent systems and applications* (pp. 315–319).

Soliman, W., Duchesne, R., Hall, W., Kennedy, M., & Tripp, C. (2021). *Capital Markets Modernization Taskforce: Final Report. Government of Ontario. Retrieved 24th April*. https://files.ontario.ca/books/mof-capital-markets-modernization-taskforce-final-report-en-2021-01-22-v2.pdf.

Song, Y., & Lu, Y. (2015). Decision tree methods: Applications for classification and prediction. *Shanghai Arch Psychiatry*, *27*(2), 130. http://dx.doi.org/10.11919/j.issn.1002-0829.215044.

Summers, S. L., & Sweeney, J. T. (1998). Fraudulently misstated financial statements and insider trading: An empirical analysis. *Accounting Review*, *73*(1), 131–146.

Tarbert, H. (2021). Self-regulation in the derivatives markets: Stability through collaboration. *Northwestern Journal of International Law & Business*, 1–37, https://www.cftc.gov/media/5596/opa_tarbertnortwesternuniversity011421/download.

van Liebergen, B. (2017). Machine learning: A revolution in risk management and compliance? *Journal of Financial Transformation*, *45*, 60–67.

van Wyk, J., & Mason, K. A. (2001). Investigating vulnerability and reporting behavior for consumer fraud victimization: Opportunity as a social aspect of age. *Journal Contemporay Crime Justice*, *17*, 328–345.

Vlasselaer, V. V., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2016). Gotcha! network-based fraud detection for social security fraud. *Management Science*, *63*(9), 3090–3110. http://dx.doi.org/10.1287/mnsc.2016.2489.

Wall, L. (2018). Some financial regulatory implications of artificial intelligence. *Journal of Economics and Business*, *100*, 55–63. http://dx.doi.org/10.1016/j.jeconbus.2018.05.003.

Whiting, D., Hanse, J., McDomand, J., Albrecht, C., & Albrecht, S. (2012). Machine learning methods for detecting patterns of management fraud. *Computational Intelligence*, *28*(4), 505–527. http://dx.doi.org/10.1111/j.1467-8640.2012.00425.x.

Williams, J. (2012). Policing the markets. In *Inside the black box of securities enforcement* (pp. 1–256). Routledge, https://doi-org.ezproxy.royalroads.ca/10.4324/9780203134887.

Williams, J. (2013). Regulatory technologies, risky subjects, and financial boundaries: governing 'fraud' in the financial markets. *Accounting, Organizations, and Society*, *38*(6–7), 544–558. http://dx.doi.org/10.1016/j.aos.2012.08.001.

Yeung, K. (2018). Algorithmic regulation: A critical interrogation- algorithmic regulation. *Regulation & Governance*, *12*(4), 505–523. http://dx.doi.org/10.1111/rego.12158.

Yokoi-Arai, M. (2007). The regulatory efficiency of a single regulator in financial services: Analysis of the UK and Japan. *Banking & Finance Law Review*, *22*(1), 23–76.