Taking the hunch out of the crunch: A framework to improve variable selection in models to detect financial statement fraud

Gepp, Adrian; Kumar, Kuldeep; Bhattacharya, Sukanto

Accounting and Finance

E-pub ahead of print: 27/10/2023

Publisher's PDF, also known as Version of record

DOI: 10.1111/acfi.13192

RESEARCH ARTICLE

ACCOUNTING & FINANCE afaanz

Taking the hunch out of the crunch: A framework to improve variable selection in models to detect financial statement fraud

Adrian Gepp[1,2] | **Kuldeep Kumar**[2] | **Sukanto Bhattacharya**[3]

[1]Bangor Business School, Bangor University, Bangor, UK

[2]Bond Business School, Bond University, Gold Coast, Queensland, Australia

[3]Deakin Business School, Deakin University, Geelong, Victoria, Australia

Correspondence
Adrian Gepp, Bangor Business School, Bangor University, Bangor, UK.
Email: adgepp@bond.edu.au

Abstract

Financial statement fraud is a costly problem for society. Detection models can help, but a framework to guide variable selection for such models is lacking. A novel Fraud Detection Triangle (FDT) framework is proposed specifically for this purpose. Extending the well-known Fraud Triangle, the FDT framework can facilitate improved detection models. Using Benford's law, we demonstrate the posited framework's utility in aiding variable selection via the element of surprise evoked by suspicious information latent in the data. We call for more research into variables that measure rationalisations for fraud and suspicious phenomena arising as unintended consequences of financial statement fraud.

KEYWORDS

Benford's law, financial statement fraud, fraud detection, fraud triangle, variable selection framework

JEL CLASSIFICATION

G32, G34

1 | INTRODUCTION

Gepp et al. (2021) estimated that financial statement fraud could be costing US$1.15 trillion worldwide, every year. This amount rises to US$1.17 trillion using recent Association of Certified Fraud Examiners (ACFE, 2022) data. Detection models can aid in the early detection of fraud to mitigate the associated cost (Gepp et al., 2021). A recent systematic review of financial statement fraud detection (Shahana et al., 2023) reveals that big data techniques such as neural networks and tree-based techniques have been, and continue to be, used for this

purpose. However, a recent study published in *The Accounting Review* (Beneish & Vorst, 2022) found such fraud detection models are too costly for auditors to use because of high false positives. This might partially explain why auditing was lagging behind in the use of big data techniques (Gepp et al., 2018), despite auditors needing to take more of a proactive approach in searching for fraud (Krambia-Kapardis, 2015). This suggests a need for an additional avenue of inquiry to produce useful financial statement fraud detection models that goes beyond just applying new data analytic techniques. Regardless of the modelling technique used, it is acknowledged in the modelling literature that the choice of input variables is an important contributor to model accuracy. Consequently, we posit that future research would benefit from theoretical guidance for selecting such variables, and develop a new framework for this purpose.

Beneish and Vorst (2022) empirically evaluated seven existing financial fraud detection models using a cost-based measure that evaluates the benefits of correctly detecting fraud relative to the cost of incorrectly alleging fraud (a false positive). The seven models included: (i) the M-score based on unweighted probit (Beneish, 1999); (ii) Cecchini et al.'s (2010) support vector machine-based model as implemented by Alawadhi et al. (2023); (iii) the F-score developed using logistic regression (Dechow et al., 2011); (iv, v) two variants that incorporate Benford's law of digit distribution (Amiram et al., 2015; Chakrabarty et al., 2022); (vi) Alawadhi et al.'s (2023) misrepresentation model; and (vii) Bao et al.'s (2020) boosted ensemble model often referred to as a machine learning model. Beneish and Vorst (2022) justified the choice of these seven models in their second footnote. For a broader coverage of models developed in prior research refer to Shahana et al. (2023).

Amongst the models not evaluated by Beneish and Vorst is one published in *Accounting & Finance* (Gepp et al., 2021) that uses a multi-technique ensemble model specifically developed for improved cost-based performance. Unfortunately the results presented by Gepp et al. (2021) in that paper are not comparable with those by Beneish and Vorst (2022) because of multiple differences, such as differing time periods and whether a matched-pairs design was used. However, consistent with the findings of Bao et al. (2020) and Gepp et al. (2021) ensemble models were found to perform best. Gepp et al.'s best overall model was a multi-technique ensemble that outperformed more than 30 other published models including both the F-score and the M-score models using a weighted error cost metric. Gepp et al. also partially answered a call from Dunstan and Gepp (2018) for more theoretically-grounded fraud detection models by choosing a large portion of the input variables with the assistance of the Fraud Triangle framework. There were three variables that were not linked to the Fraud Triangle; all compared financial and non-financial information with a large difference being suspicious.

Because the initial selection of input variables is a crucial step in constructing effective fraud detection models (Gepp et al., 2021), a theoretical framework guiding the process would be very valuable for future research. The earlier finding by Perols and Lougee (2011) is still true: the initial selection of variables in financial statement fraud detection research is not standardised by any consistent, underpinning theoretical framework. A recent study by Xu et al. (2022) did use the GONE framework (based on Greed, Opportunity, Need, and Exposure) to guide variable selection in their development of machine learning models to predict corporate fraud in China. However, this framework does not leverage the fact that most frequently input variables are chosen based on prior research findings and the Fraud Triangle (Shahana et al., 2023). Despite the Fraud Triangle arguably being a prime candidate to provide the necessary theoretical guidance in this regard, it still falls short as demonstrated above with Gepp et al.'s (2021) study. The reason is that the Fraud Triangle solely focuses on the precursor conditions that drives fraudulent behaviour rather than operationalisable indicators for fraud detection. Thus, the Fraud Triangle is not oriented to the detection of financial statement fraud and guiding variable selection for modelling. Consequently, this work is motivated by an academic, as well as a practical, need to suitably extend the Fraud Triangle to make it suitable for providing

the necessary theoretical guidance for input variables selection when constructing a financial statement fraud detection model. Our research question is whether such a framework can be developed.

Bao et al. (2020) explored a new approach regarding input variables. Instead of using a set of accounting ratios and other variables expertly selected by the researchers, 28 accounting data points were used in raw form. Bao et al. argued their approach avoided bias associated with ratio selection. This approach showed some promise (Bao et al., 2020), but the resulting model was still not good enough to be useful in practice (Beneish & Vorst, 2022). Thus, we propose an alternative approach that is more theoretically guided. This approach utilises domain-specific knowledge about the problem (in this case, financial statement fraud), which has generally been recommended to compile a better list of input variables (Guyon & Elisseeff, 2003). While this arguably could introduce bias, the issue is largely mitigated with the use of a suitable theoretical framework to guide variable selection, such as the one proposed in this paper.

The remainder of this paper is structured as follows. Section 2 briefly reviews the Fraud Triangle and key related theories, before in Section 3, we propose "suspicious information" as an additional factor and develop the Fraud Detection Triangle (FDT) that can guide variable selection in financial statement fraud detection models. In Section 4, we offer a numerical demonstration of the posited framework's utility before concluding in Section 5.

2 | THE CLASSIC FRAUD TRIANGLE FRAMEWORK AND SOME EXTENSIONS

Drawing from the work of Cressey (1953), the classic Fraud Triangle framework is a well-known conceptual framework to understand what drives fraudulent behaviour (Morales et al., 2014). The Fraud Triangle posits that frauds share three factors (see Figure 1). The *Opportunity* factor requires fraudsters to perceive an opportunity to commit fraud. Examples pertaining to financial statement fraud include weak internal control systems such as no segregation of duties, weak corporate governance and poor audit quality. The *Pressure* factor requires fraudsters to perceive a pressure to commit fraud, and that they cannot seek help or share their problem (Dorminey et al., 2012). Examples include pressure to meet or exceed analysts' earnings expectations, cash flow problems and restrictive debt covenants. The *Rationalisation* factor is about having an excuse within the fraudster's personal moral comfort zone (Dorminey et al., 2012), or more formally, an attempt to reduce the cognitive dissonance within the individual (Ramamoorti, 2008). Example rationalisations include "We will make it up next financial year" and "It is best for the company".

The Fraud Triangle is included in almost all industry and academic education on fraud (Dorminey et al., 2012) even being embedded in professional auditing standards (Free, 2015). Nevertheless, a number of shortcomings have been uncovered and additional models (or extensions) have been proposed and are briefly discussed below.

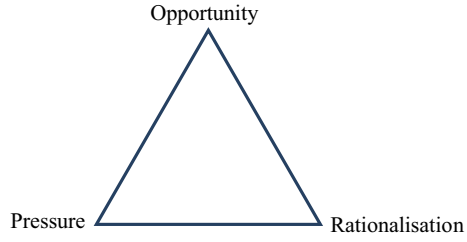

FIGURE 1 Classic Fraud Triangle framework.

2.1 | Capability

Wolfe and Hermanson (2004) contend the fraudster also needs the necessary capabilities to execute the fraud and so proposed a fourth factor, capability, thereby constructing the Fraud Diamond. Kassem and Higson (2012) also added capability as a fourth factor to their New Fraud Triangle model, while Dorminey et al. (2012) incorporated it within the opportunity factor.

2.2 | Incentives

In the infamous Tyco financial statement fraud case, instead of a pressure there was a strong incentive: executives made US$430 million from inflating the share price by publishing fraudulent information (Dorminey et al., 2012). This has been addressed by expanding pressure to include a broader set of incentives according to the acronym MICE (Money, Ideology, Coercion and Ego or Entitlement; Kranacher et al., 2011). Although MICE has been deemed an incomplete explanation of fraud motivations (Dorminey et al., 2012), it nevertheless provides additional considerations.

2.3 | Attitudes and integrity

The Fraud Scale proposed by Albrecht et al. (1984) replaced rationalisation with personal integrity. The importance of personal integrity is reinforced by Rezaee and Riley (2010). Attitude has also been considered part of rationalisation (Brazel et al., 2009; Lou & Wang, 2009). Examples of an attitude and a lack of personal integrity that assists in rationalising fraud are respectively that "The rules don't apply to me" and "What I want is more important than honesty". Krambia-Kapardis (2022) recently noted that corporations can themselves be economic criminals and so we should also consider the attitudes and integrity of corporations and corporate officers.

2.4 | Conditions, culture and choice

Rezaee and Riley (2010) used the 3Cs models for studying financial statement fraud according to which, a fraud occurs if there are:

1. favourable *conditions* such as pressures and incentives, and opportunities to commit fraud;
2. a corporate *culture* that provides the opportunity and motivations for senior management to commit fraud; and
3. senior management who make the *choice* to commit fraud and rationalise it.

This framework is largely a different grouping of factors similar to those in the Fraud Triangle and so is still not oriented towards guiding variable selection for fraud detection models. Ramamoorti (2008) also stated that frauds can occur because of an individual, colluding individuals or broad cultural or societal influences. Free et al. (2007) and Boulter et al. (2013) suggested that fraud at an organisational level is underpinned by culture, leadership and subverted management controls. These factors are arguably already covered by the pressure, incentives and opportunity factors, but consistent with

Krambia-Kapardis (2022), these papers highlight the need to think more broadly than a single corrupt person. Furthermore, the majority of occupational frauds involve collusion and those that do are more costly (ACFE, 2022). Given that collusive frauds generally cannot be prevented using traditional controls, detection models could be useful in uncovering them (Silver et al., 2008).

Let us now consider a few studies that have explicitly drawn insight from the Fraud Triangle when developing a financial statement fraud detection model. Lou and Wang (2009) considered all three factors using Taiwanese data, as did Skousen and Wright (2008) and Skousen et al. (2009) using US data. However, there was considerable entanglement between the three factors and the extent to which the framework offered constructive guidance remains questionable. In contrast, Brazel et al. (2009) considered two factors (excluding rationalisation) and a new "suspicious accounting" factor without defining it. However, this new factor only considered accounting information that, arguably, could be classified into one of the original factors. For example, total accruals were considered in this new factor, but accruals are easier to manipulate than cash that is easier to audit, and so higher accruals represent a greater fraud *opportunity*. Further, prior positive accruals reduce ways to legitimately manage earnings and so may increase the *pressure* to commit fraud to avoid accrual reversals or maintain accrual growth (Beneish, 1997; Perols & Lougee, 2011). Overall, the use of different variable categories renders it difficult to make comparisons and the Fraud Triangle is at best providing rather tenuous theoretical guidance for constructing effective financial statement fraud detection models.

3 | DEVELOPING THE FRAUD DETECTION TRIANGLE FRAMEWORK: EXTENDING THE FRAUD TRIANGLE TO FOCUS ON DETECTION

One way to detect fraud is to search for its underlying drivers or motives, which is addressed in Section 3.1 by enhancing the existing factors of the Fraud Triangle. Another way to detect fraud is by discovering unusual patterns that occur as unintended consequences of fraud (and its concealment), which is captured with the new S factor proposed in Section 3.2. These are then integrated to form the new Fraud Detection Triangle in Section 3.3. An additional theoretical basis for the primary novelty of this framework, the S factor, is then detailed in Section 3.4.

3.1 | Enhancing the three original factors

The following factors are enhancements to the Fraud Triangle factors based on the additional research findings presented in Section 2.

3.1.1 | *Exploitable* opportunity (O) factor

Opportunities to commit fraud are only enacted if there are people with the capability of exploiting them (Dorminey et al., 2012). Thus, consistent with Dorminey et al. (2012) and Wolfe and Hermanson's (2004) additional capability factor is incorporated into the opportunity factor in the newly proposed framework. The addition of *exploitable* indicates an opportunity existing in the presence of a single person or multiple people with the capability of exploiting that opportunity; thus, it applies to both individual and collusive frauds.

3.1.2 | Pressure/incentive (I) factor

A broader definition of the pressure factor that includes incentives and MICE is used in the newly proposed framework. This is similar to Dorminey et al. (2012) and Kassem and Higson (2012). Money is captured by financial pressure and incentives, while coercion is captured by pressures that come from managers. Ego and ideology are both captured by including incentives as well as pressures. It is worth noting that both Ego and Ideology probably also play a role in rationalisation, and will likely be influenced by organisational culture (Boulter et al., 2013). It is also important to note that this factor encompasses the pressures and incentives regarding both individual and collusive frauds.

3.1.3 | Integrity/attitude/rationalisation (R) factor

This factor incorporates rationalisations, attitudes and integrity of individual fraudsters, colluding individuals (Ramamoorti, 2008; Silver et al., 2008), and corporations and corporate officers (Krambia-Kapardis, 2022). While considering common characteristics of fraudsters is useful, we must remember to remain flexible because the heterogeneity involved means that a single common profile of fraudsters is not feasible (Krambia-Kapardis, 2016, 2022). Notably, no further changes are made based on the 3Cs model (Rezaee & Riley, 2010) because: (i) this R factor addresses the choice to commit fraud; (ii) the new O and I factors incorporate favourable conditions; and (iii) a corporate culture that provides the opportunity and motivation for fraud are addressed in the O and I factors.

3.2 | A new additional factor – suspicious information (S)

We posit a suspicious information or S factor focused on detection, in addition to the O, I and R factors just presented that focus on the drivers of fraud. The proposed S factor encompasses detectable unintended consequences (or data spinoffs) that occur as a result of an occurrence of fraud and any concerted effort to conceal it. These consequences, unintended by the fraudsters, affect the way financial information is presented. For example, such unintended consequences can affect the statistically expected patterns in reported numbers, thereby enabling pattern recognition models to detect these anomalies as suspicious and indicating a higher likelihood of fraud. The use of Benford's law is a prime example, whereby the distribution of digits in naturally occurring numbers follow this non-uniform pattern. Numbers in financial statements that deviate from Benford's law are indicative of a higher risk of fraudulent manipulation (Bhattacharya et al., 2011) and thus contain potentially valuable information for detection models. However, such a variable is not justified within the existing factors that focus on the drivers of fraud. Deviations from Benford's law are not indicative of changes in exploitable opportunities, pressures and incentives or rationalisations, but it is suspicious information that can assist in the detection of financial statement fraud. This focus on detection is the key element of the proposed S factor.

Consider a company experiencing rapid financial growth. It would be expected to also have growth in non-financial variables (Brazel et al., 2009). For example, changes in sales (or assets) are expected to be positively correlated with changes in the number of employees. If sales were increasing despite a stable employee base, then this zero correlation can be considered suspicious because the fast-growing financial information is easier to fraudulently manipulate than the non-financial information that is relatively easy to definitively verify. This information does not relate to an exploitable opportunity (O), a pressure or incentive (I) or a rationalisation, integrity or attitude issue (R). Thus, it could be missed without the addition of the new

S factor. There are also other examples of fraud indicators that are not guided by any of the existing O, I and R factors or their latter extensions, but find support within the new S factor:

- A chief executive officer (CEO) being unanimously dismissed by the board of directors approximately 2 weeks after being appointed is suspicious, particularly if the initial reasons given are vague. This might occur if the board found out the CEO had committed fraud, although in the case of Olympus, the reason was that the CEO was a whistle-blower about the financial statement fraud.
- Enron acquired the naming rights for a baseball stadium (Enron Field) in a US$100 million deal. Such an expense is suspicious as the common justification of improving the retail customers' image of the company did not apply as Enron was primarily not a retail company. The former CFO of Enron now considers this to be a suspicious action (Fastow, 2016).
- Anecdotal evidence from fraud practitioners indicate that it is suspicious when employees do not take leave, and thus another person never completes their work, even temporarily (ACFE, 2013). This can be useful for a fraudster not wanting another employee discovering their fraud.
- Common fraud red flags used by non-professional investors are high management turnover, violation of debt covenants, SEC investigation commencement and pending litigation (Brazel et al., 2015). These can be considered suspicious, but unfortunately, Brazel et al. (2015) note that these warnings mostly occur in the latter stages of frauds.
- Larger returns relative to the average assets in the prior 2 years have been linked with higher fraud risk (Gepp et al., 2021). This empirical finding is consistent with the S factor as large profits generated from a historically relatively low asset base can be suspicious in terms of potentially fraudulently inflated profits.

The above examples would be overlooked if only the O, I and R factors were considered. This helps demonstrate the need for the S factor to specifically consider suspicious information revealed that may indicate a fraud has occurred.

3.3 | Embedding the S factor within the new Fraud Detection Triangle (FDT) framework

The proposed FDT framework retains the previous structure and contents of the classic Fraud Triangle and builds an extra element into it (see Figure 2). The FDT framework incorporates the prior extensions of the pre-existing O, I and R factors (see Section 3.1) that capture the drivers of fraud, as well as the new suspicious information (S) factor focused on the detectable unintended consequences of fraudulent behaviour. This is why the new framework contains the word detection. The Fraud Detection Triangle (FDT) posits that whenever a financial fraud is committed via the interplay of the O, I and R factors, an *information handprint* is likely left behind by the perpetrator. To the extent that this handprint evokes an element of surprise (and hence suspicion) regarding fraudulent manipulation latent in the data, it can be of use to forensic investigators.

There is no requirement for all the factors in the framework to be present; if any single factor is present then there is an increased fraud concern. This is consistent with the modern usage of the original Fraud Triangle. Professional accounting bodies have contended that the presence of only one triangle factor is enough for fraud to occur (Skousen et al., 2009); for example, Dorminey et al. (2012) point out that fraudsters with a predatory nature only require an opportunity to commit a fraud. Andon et al. (2015: 35) also state that all factors are not required and Boulter et al. (2013) mathematically demonstrated that the three original factors are inherently inter-linked and consequently one factor can predispose the presence of the other two.

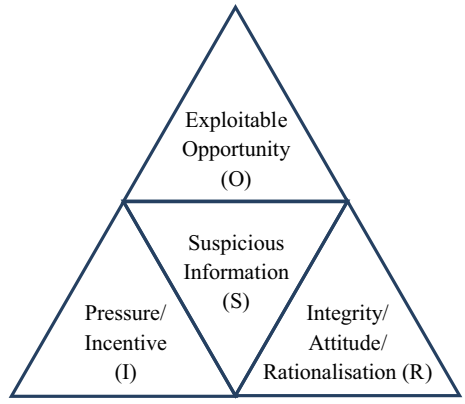

FIGURE 2 The new Fraud Detection Triangle (FDT) framework. It is acknowledged that the layout of this diagram is similar to the model presented by Kassem and Higson (2012).

New financial statement fraud detection modelling studies can use the FDT framework to motivate and guide the initial selection of input variables. In a recent study, Gepp et al. (2021) identified 47 variables that were publicly available, had empirical support from prior research and a rationale for their influence on financial statement fraud. Where possible, each variable was linked to at least one factor of the Fraud Triangle, which directly map to the new FDT's O, I and R factors. Notably, the variables that could not be linked correspond directly to the FDT's new S factor.

By using the FDT framework, under-researched factors that require more and better variables to measure them can be identified. Thus far, more emphasis has been given to the O and I factors relative to the R factor (Gepp et al., 2021). This is despite the importance of the rationalisation factor (Krambia-Kapardis, 2001) and probably because it is the most difficult factor to measure (Skousen et al., 2009). For example, Gillett and Uddin (2005) found that while the attitude of the chief financial officer (CFO) is important, the CFO's compensation is not a useful proxy. Consequently, we join the call (Free, 2015; Gepp et al., 2021; Trompeter et al., 2013) for further research into variables measuring the R factor.

Because it is a newly proposed additional angle to the Fraud Triangle framework, future empirical research is expected to discover the true value of the S factor. The recent poor performance of financial statement fraud detection models (Beneish & Vorst, 2022) and paucity of recent modelling breakthroughs that have been able to make the headlines are perhaps an indication of being close to saturation with regard to financial statement fraud detection research with just the O and I (and to a lesser extent the R) factors to rely on for theoretical guidance. Armed now with the S factor for drawing theoretical sustenance, we hope experts will produce a fresh crop of research on financial statement fraud detection modelling to advance the literature.

3.4 | Theoretical basis of the new S factor – drawing from mathematical information theory

Ndofor et al. (2015) claim that opportunities to commit financial fraud are principally determined by the presence of information asymmetries between top management and other stakeholders. When top management takes advantage of such information asymmetries to commit fraud, this paper posits that they commonly, perhaps even inevitably, leave a detectable unintended handprint which is captured by the new S factor. Such detectable handprints

result in an element of surprise (mathematically captured as entropy) from a set of red-flagged transactions that are suspected to conceal a fraud.

The S factor draws theoretical sustenance from the concept of entropy in mathematical information theory (Shannon, 1948). For a complete set of $j = 1, 2, \ldots, k$ reported account balances at a given point in time, the S factor is mathematically interpretable as the sum-product of the probability p_j and $\log_b(p_j)$, where p_j is the probability of the jth account balance showing a spurious amount in the auditor's expert opinion, meaning it is suspicious. Consistent with a standard information-theoretic approach, setting $b = 2$ yields a measure of binary information, where the binary event is whether (coded as 1) or not (coded as 0) the jth account balance shows a spurious amount. The practical utility of such an entropy measure has already been computationally demonstrated for financial fraud detection systems (Bhattacharya et al., 2011).

Given that an account cannot be simultaneously *suspicious* and *not suspicious* in the same auditor's view, we develop a formalisation of the S factor via a standard logit model as follows:

$$\log_2\left[p_j / \left(1 - p_j\right)\right] = \beta_0 + \beta_1\Omega + \beta_2\vartheta + \beta_3\Psi, \tag{1}$$

$$\text{i. e. } p_j / \left(1 - p_j\right) = 2^{\left(\beta_0 + \beta_1\Omega + \beta_2\vartheta + \beta_3\Psi\right)}. \tag{2}$$

Here, Ω, ϑ and Ψ are the respective factor operationalisations of the three extant vertices of the classical fraud triangle i.e. O, I and R. Applying the usual algebraic process yields as follows:

$$p_j = 2^{\left(\beta_0 + \beta_1\Omega + \beta_2\vartheta + \beta_3\Psi\right)} - p_j 2^{\left(\beta_0 + \beta_1\Omega + \beta_2\vartheta + \beta_3\Psi\right)}, \tag{3}$$

$$\text{i. e. } p_j = 2^{\left(\beta_0 + \beta_1\Omega + \beta_2\vartheta + \beta_3\Psi\right)} / \left(1 + 2^{\left(\beta_0 + \beta_1\Omega + \beta_2\vartheta + \beta_3\Psi\right)}\right), \tag{4}$$

$$\text{i. e. } p_j = 1 / \left(2^{-\left(\beta_0 + \beta_1\Omega + \beta_2\vartheta + \beta_3\Psi\right)} + 1\right). \tag{5}$$

Denoting an estimated measure of S as $\mathfrak{Z}$ and drawing from the entropy formulation as exposited by Bhattacharya et al. (2011), an information theoretic formalisation of S is:

$$\mathfrak{Z} = \sum_j \left(p_j \log_2 p_j\right), \tag{6}$$

$$\text{i. e. } \mathfrak{Z} = \sum_j \left[1 / \left(2^{-\left(\beta_0 + \beta_1\Omega + \beta_2\vartheta + \beta_3\Psi\right)} + 1\right) \log_2 \left\{1 / \left(2^{-\left(\beta_0 + \beta_1\Omega + \beta_2\vartheta + \beta_3\Psi\right)} + 1\right)\right\}\right]. \tag{7}$$

The estimates of p_j are derivable from a series of logit models with the factor operationalisations of the extant fraud triangle vertices (i.e., Ω, ϑ and Ψ) as explanatory variables.

Therefore, the S factor as mathematically formalised above, can theoretically go beyond the identification of the red flags in standard practice by auditors. In effect, once a red flag has been located via the standard audit process, the presence of S enables the computation of an expected information value for that red flag, which is the mathematical equivalent of the element of surprise that will be generated if that identified account balance does indeed contain a spurious figure. This can help operationalise a useful input variable in a fraud-detection model to identify any latent pattern underlying a whole set of standard red flags. This carries practical usage value by helping to determine what would be the most economical approach for fraud detection given the quantum of surprise involved, as deduced from the patterns uncovered in

a dataset. The next section uses synthetic datasets to demonstrate the FDT framework's utility in aiding key variable selection via the element of surprise evoked by suspicious information deduced from patterns latent in the data.

The S factor also provides a theoretical basis for the inclusion of complex interactions between input variables that have no theoretical foundation in the existing O, I and R factors. For example, the amount of new stock issued could be insignificant regarding an incentive to fraudulently increase the share price, but it might be significant as suspicious information in terms of its interaction with recent changes in the sales level and the composition of assets. With the S factor providing a theoretical basis, such complex interactions between variables can be modelled using modern techniques such as decision trees. Davis and Pesch (2013) claim that there is no one-size-fits-all solution for fraud detection and that uniform approaches to detection may be inappropriate. Such non-uniformity can be achieved through detection models considering complex interactions between variables as part of the S factor. For example, including organisation type and social influence ability in a tree-based model would allow fraud detection to be contingent on these characteristics.

Overall, the key contribution of the S factor is embedding a detector-focused factor in addition to the classic Fraud Triangle factors that measure fraud drivers. This enables the inclusion of input variables that are not related to drivers of fraud, but might reveal suspicious patterns potentially occurring as the consequence of some latent fraudulent behaviour.

4 | BRINGING THE S FACTOR INTO PLAY – AN ILLUSTRATIVE MODEL USING BENFORD'S LAW

Benford's law has been too widely applied in the context of fraud to be meaningfully reviewed here; interested readers are directed towards readings such as Bhattacharya et al. (2011), Stambaugh et al. (2012), Nigrini (2017) and Rad et al. (2021). Notably, Benford's law is not without its limitations and questions have been raised about its propensity to generate too many false negatives when used for fraud detection. Goodman (2016) argued that it is perilous to claim whether or not a dataset conforms to Benford's law based on statistical tests that make a priori assumptions about the distributional error that may not be consistent with the actual error associated with conformance to Benford's law. Cho and Gaines (2007) suggest a non-parametric alternative that addresses this issue, but do not provide a benchmark cut-off point beyond which a dataset could be confidently claimed to be non-conforming to Benford's law.

Going back to the theoretical description of the S factor, non-conformance with Benford's law needs to convey an element of surprise to evoke suspicion of fraudulent manipulations being latent in the data. Accordingly, auditors and forensic investigators would need to consider the expected information content conveyed by the non-conformance. It is this expected information content that is the element of surprise, and that forms our S factor. We provide a relatively straightforward computational illustration, using entropy as a numerical measure of expected information to better exposit the S factor.

Consistent with the validated methodology in prior research (Bhattacharya et al., 2011; Busta & Weinberg, 1998), we evaluate how well a statistical distinction can be made between non-contaminated (i.e., Benford's law-derived) and contaminated (i.e., non-Benford) data. Specifically, we construct several datasets with varying levels of *contamination*: each of the constructed datasets includes, in varying proportions, numbers randomly drawn from a Benford distribution as well as three non-Benford distributions: uniform, bell (normal) and a Hill distribution (Bhattacharya et al., 2011). For the sake of expositional simplicity, we collapse the three (O, I, R) factor operationalisations into a single factor: an integer between 1 and 9 (illustratively representing the first digit of an account balance or transaction record) selected at random from datasets constructed from varying proportions of numbers

drawn from Benford and non-Benford distributions. The outcome variable is binary, with 0 indicating that the selected number belongs to the Benford distribution, and 1 indicating it does not. A logit model is fitted to each of the datasets with the pertinent results presented below. Our expectation is that there ought to be a crossover point where the level of contamination allows the logit model to return a statistically significant regression coefficient, while still conveying an element of surprise in the sense that the proportion of contamination in the dataset is neither too high (making it an overkill to apply any computational model) or too low (increasing the false positives to the point of a prohibitive cost implication). The results of the logit models for datasets each with 500 numbers at varying levels of contamination (i.e. proportion drawn from the non-Benford distributions) are presented in Tables 1–5.

It is evident from Tables 1–5 that the logit coefficients are highly statistically significant in all cases, meaning it is possible to systemically distinguish between the numbers belonging to Benford and non-Benford distributions. However, interesting insights emerge when we compute the expected information content, as measured by the entropy values for each datasets (see Tables 6–10), as well as the incremental entropy values across the five datasets (see Tables 11–14).

TABLE 1 Logit model with 10% contamination level.

	Coefficient	Std error	Wald test statistic (1 df)	*p*-Value
X 10 percent	0.332	0.076	19.294	<0.001
Constant	0.831	0.308	7.281	0.007

TABLE 2 Logit model with 25% contamination level.

	Coefficient	Std error	Wald test statistic (1 df)	*p*-Value
X_25_percent	0.236	0.047	25.173	<0.001
Constant	0.097	0.213	0.206	0.650

TABLE 3 Logit model with 50% contamination level.

	Coefficient	Std error	Wald test statistic (1 df)	*p*-Value
X_50_percent	0.199	0.038	26.830	<0.001
Constant	−0.861	0.184	21.860	<0.001

TABLE 4 Logit model with 75% contamination level.

	Coefficient	Std error	Wald test statistic (1 df)	*p*-Value
X_75_percent	0.221	0.042	27.164	<0.001
Constant	−2.057	0.221	86.948	<0.001

TABLE 5 Logit model with 90% contamination level.

	Coefficient	Std error	Wald test statistic (1 df)	*p*-Value
X_90_percent	0.208	0.056	13.821	<0.001
Constant	−3.136	0.314	99.734	<0.001

TABLE 6 Expected information for data with 10% contamination.

Digit	10% Non-Benford (prob. value from fitted logit model)	Entropy value
1	0.051	0.2906
2	0.062	0.3353
3	0.075	0.3843
4	0.091	0.4398
5	0.109	0.4969
6	0.131	0.5602
7	0.157	0.6271
8	0.186	0.6930
9	0.220	0.7602
	Average value across all nine digits	0.5097

TABLE 7 Expected information for data with 25% contamination.

Digit	25% Non-Benford (prob. value from fitted logit model)	Entropy value
1	0.138	0.5790
2	0.166	0.6485
3	0.199	0.7199
4	0.236	0.7883
5	0.279	0.8541
6	0.325	0.9097
7	0.775	0.7692
8	0.428	0.9850
9	0.483	0.9992
	Average value across all nine digits	0.8059

TABLE 8 Expected information for data with 50% contamination.

Digit	50% Non-Benford (prob. value from fitted logit model)	Entropy value
1	0.340	0.9248
2	0.386	0.9622
3	0.434	0.9874
4	0.484	0.9993
5	0.534	0.9967
6	0.583	0.9800
7	0.630	0.9507
8	0.675	0.9097
9	0.717	0.8595
	Average value across all nine digits	0.9523

TABLE 9 Expected information for data with 75% contamination.

Digit	75% Non-Benford (prob. value from fitted logit model)	Entropy value
1	0.582	0.9805
2	0.638	0.9443
3	0.691	0.8920
4	0.739	0.8283
5	0.782	0.7565
6	0.819	0.6823
7	0.852	0.6048
8	0.879	0.5322
9	0.902	0.4626
	Average value across all nine digits	0.7426

TABLE 10 Expected information for data with 90% contamination.

Digit	90% Non-Benford (prob. value from fitted logit model)	Entropy value
1	0.762	0.7917
2	0.817	0.6866
3	0.862	0.5790
4	0.897	0.4784
5	0.924	0.3879
6	0.944	0.3114
7	0.959	0.2469
8	0.970	0.1944
9	0.979	0.1470
	Average value across all nine digits	0.4248

TABLE 11 Change in entropy between 10% and 25% contaminated datasets.

Digit	Δ Entropy value (%)
1	99.21
2	93.38
3	87.33
4	79.25
5	71.89
6	62.40
7	22.66
8	42.13
9	31.44
Average change across all nine digits	65.52

TABLE 12 Change in entropy between 25% and 50% contaminated datasets.

Digit	Δ Entropy value (%)
1	59.73
2	48.37
3	37.15
4	26.76
5	16.69
6	7.73
7	23.59
8	−7.64
9	−13.98
Average change across all nine digits	22.05

TABLE 13 Change in entropy between 50% and 75% contaminated datasets.

Digit	Δ Entropy value (%)
1	6.02
2	−1.85
3	−9.66
4	−17.11
5	−24.10
6	−30.38
7	−36.38
8	−41.50
9	−46.18
Average change across all nine digits	−22.35

TABLE 14 Change in entropy between 75% and 90% contaminated datasets.

Digit	Δ Entropy value (%)
1	−19.26
2	−27.29
3	−35.09
4	−42.24
5	−48.72
6	−54.36
7	−59.18
8	−63.48
9	−68.22
Average change across all nine digits	−46.43

For the lowest level of contamination (10% in Table 6), as the distribution is very close to Benford, the likelihood of a larger digit belonging to a non-Benford distribution gets progressively higher. This is because larger digits have a lower frequency of occurrence according to Benford's law, and these data are very close (90%) to Benford. The higher digits are also associated with higher entropy values and evoke a stronger element of surprise given the low contamination. For Table 7, as a quarter of the numbers are drawn from non-Benford distributions, the element of surprise (entropy) associated with the lower digits increases relative to the 10% contaminated data. This agrees with intuitive logic, as it is now slightly less likely that the lower digits originated from a Benford distribution. However, the entropy values associated with the higher digits are still higher than the lower digits because numbers drawn from a Benford distribution (75%) still dominate.

For the 50% contaminated dataset, the element of surprise associated with the lower digits increases again (relative to the previous 25% contaminated dataset). However, the rate of increase is smaller than before, as can be seen by comparing the percentage change in entropy values between Tables 11 and 12. The average entropy across all nine digits is maximised at 50% contamination (which agrees with information theoretic logic), marking a critical contamination limit. It is critical because the marginal benefit of using detection models (such as logit or neural networks) becomes low above 50% contamination as the systemic issue should become visually apparent to an expert investigator. At the high levels of contamination (75% and 90%), there is very little element of surprise conveyed by the logit models as shown in Tables 9 and 10 by the steadily falling entropy value across all the nine digits.

Moving from 10% to 25% contamination (Table 11), the average change in entropy is 65.52% across all digits, with higher percentage change in the lower digits as is expected given Benford's distribution entails a higher relative frequency of the lower digits. The change in entropy is positive for all nine digits, which implies that at this stage there is enough surprise imparted by the extra contamination to evoke suspicion. The average change in entropy then drops to 22.05% (Table 12) when moving from 25% to 50% contamination. The change is actually negative for the two highest digits (8 and 9), so the extra contamination does not translate into as much surprise although it is still enough to evoke suspicion as the overall change is positive (22.05%). Increasing contamination beyond 50% results in a negative average change in entropy (−22.35% and −46.43% in Tables 13 and 14 respectively), indicating that at 75% and 95% contamination levels; no element of surprise is left to make it meaningful for fraud detection as it will already be apparent to an expert. Thus, the crossover point in this case would be somewhere between 50% and 75% contamination. At lower levels of contamination, the cost of false positives might become too prohibitive, while at higher levels complex fraud detection models become a strategic overkill as experts can already uncover it.

As a caveat to the reader, it needs to be stated that the above numerical illustration is not intended as a robust empirical validation of the FDT framework's new suspicious information (S) factor. Rather, it is intended to numerically demonstrate how the element of surprise, as measured by the expected information content conveyed by a data analytical method, could help assess that method's practical utility for fraud detection, balancing strategic overkill and too many costly false positives. This expected information content could also help determine whether newer input variables were needed.

5 | CONCLUSIONS, KEY LIMITATION AND CALL FOR FUTURE RESEARCH

Financial statement fraud continues to be a costly problem. Auditors have been tasked with being more proactive (Krambia-Kapardis, 2015) and fraud detection models could help, but

Beneish and Vorst (2022) have largely found existing models to be unsuitable for use in practice. In addition to continuing to explore new modelling techniques, we propose a new approach to improving financial statement fraud detection models with a theoretically guided selection of input variables. Selecting the most appropriate variables is a key decision, yet it is not standardised by a common framework in prior financial statement fraud modelling research. Thus, the new Fraud Detection Triangle (FDT) framework has been developed and is proposed for this purpose. The FDT framework indicates that the likelihood of financial statements being fraudulent increases with either (or both)

- the presence of any of the drivers of fraud: Exploitable Opportunity (O factor), Pressure/Incentive (I factor) or Integrity/Attitude/Rationalisation (R factor); and
- the presence of Suspicious information (new S factor) that has occurred as an unintended consequence of fraud and the attempts to conceal it.

Unlike in other frameworks, the addition of the S factor allows for the fact that fraud can sometimes be detected from identifying unusual patterns that occur as an unintended consequence of fraud, regardless of whether the preceding drivers of fraud are detectable or not.

The new FDT framework can play a role as an overall theory to assist in guiding the selection of variables for future financial statement fraud detection research. This provides a new approach in the search for more accurate detection models and its consistent use would improve comparability between research studies. Prior research has identified publicly available variables (see Section 3.3) that initially operationalise each factor of the FDT framework, but additional multivariate research is needed to determine the best variables. Studies that investigate additional variables that measure R and S factors would be particularly helpful to freshen up the literature as less focus has been placed on them in prior research. The biggest limitation of this research is the lack of empirical validation of the efficacy of variables drawing theoretical guidance from R and S factors, rather than the more common O and I factors. As future researchers use the new FDT framework to guide variable selection, a full evaluation of the framework will be possible by assessing whether the resulting models are notably better at detection.

5.1 | Call for additional research into the R and S factors

Given it is a new factor, further research into variables that measure the S factor is needed. Current variables account for frequent changes in the CEO or CFO being potentially suspicious, but it is conceivable that fraud results in unusually high employee turnover beyond just these positions, as investors follow changes in management more broadly (Brazel et al., 2015). As mentioned in Section 3.2, the following potential measures of the S factor also warrant future research: the number of employees with unusually low usage of leave, early indications of SEC investigations or other related litigation, and the presence of unusual, large expenditures such as sport-related naming rights for non-retail businesses or disproportionately expensive executive retreats. With the increased availability of digital information, some of this previously difficult-to-obtain information may now be obtainable.

Multi-disciplinary opportunities also exist for variables that measure the S factor by utilising research from mathematics and information anomalies. Information theory underpins the new S factor from a theoretical perspective. There is a further opportunity to develop variables that empirically capture the element of surprise in manipulated figures using the sum-product formula for entropy (see Section 3.4) and then empirically evaluate them in a detection model spanning all FDT framework factors. We also renew an earlier call from Amershi and Feroz (2000) for further research into whether numbers of mathematical significance such as Golden and Silver Means are useful for fraud detection. While Benford's law has been

well-studied on its own, its effectiveness has not been evaluated in a fraud detection model that spans all four FDT framework factors.

Prior research has concluded that there is a key socio-cultural dimension to fraud that may assist in identifying distinctive features, but that it has largely been ignored in previous Fraud Triangle based research (Free & Murphy, 2015; Kumar et al., 2018; Murphy & Free, 2016). These features include measures of organisational culture and ethical climate as underlying drivers of the R factor. Additionally, deviances from usual social behaviours could be incorporated into the new S factor. The challenge for researchers is obtaining publicly available proxies for the socio-cultural dimension of suspicious information. The solution will likely require a multi-disciplinary approach involving accounting and auditing, as well as behavioural and systems sciences.

Better measures of executive attitude (or integrity) would be valuable regarding the R factor, particularly because EY (2016) found that 42% of executives could justify unethical behaviour to meet financial targets. Analysis of earnings conference calls could yield useful indicators of the ability to rationalise fraud, such as searching for vocal dissonance markers (Hobson et al., 2011). An example of a useful linguistic cue is the use of more pleasantness and less lexical diversity being associated with fraud (Humpherys et al., 2011). Furthermore, Shafer et al. (2016) recently found that Chinese tax accountants with higher levels of professional commitment viewed fraud as more unethical and were less inclined to commit fraud, likely because it would be harder to rationalise. It would be valuable for future researchers to test such measures of professional commitment for measuring the R factor.

Researchers (Cohen et al., 2011; Murphy, 2012) have also demonstrated that certain personality traits are associated with fraud. The question is how best to incorporate such information into fraud detection models. Using the hack and subsequent public release of Ashley Maddison data, Griffin et al. (2016) showed that executives who used Ashley Maddison to facilitate extramarital affairs were more likely to commit corporate fraud. We hypothesise that someone who is personally unfaithful can more easily rationalise corporate fraud. This indicator cannot be used as it is usually private, but it does demonstrate that measures of the R factor need not be limited to the corporate setting. Sentiment analysis is a growing area of research in accounting and finance (Gepp et al., 2018) and one idea for measuring the R factor is to develop ethical (or personality) sentiment scores for executives using public information (both corporate and personal). Sentiment analysis could also be considered in many other ways. For instance, large variations in the online sentiment about a company might be considered suspicious and operationalise the S factor.

ACKNOWLEDGEMENTS

The authors thank the participants and reviewers at multiple conferences: American Accounting Association Annual Meeting, Asia-Pacific Interdisciplinary Research in Accounting Conference AFAANZ Conference and the Asian-Pacific Conference on International Accounting Issues.

DATA AVAILABILITY STATEMENT

The synthetic data that supports the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Adrian Gepp https://orcid.org/0000-0003-1666-5501

REFERENCES

ACFE. (2013) *Financial statement fraud conference*. Chicago, IL: Association of Certified Fraud Examiners (ACFE).

ACFE. (2022) *Report to the nations on occupational fraud and abuse*. Reportno. Report Number|, Date. Place Published|: Institution|.

Alawadhi, A., Karpoff, J., Koski, J.L. & Martin, G.D. (2023) *The prevalence and price distorting effects of undetected financial misrepresentation: empirical evidence*. Working Paper. Available from: https://ssrn.com/abstract=3532053 [Accessed 2nd May 2023].

Albrecht, W.S., Howe, K.R. & Romney, M.B. (1984) *Deterring fraud: the internal auditor's perspective*. Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.

Amershi, A.H. & Feroz, E.H. (2000) The occurrence of fibonacci numbers in time series of financial accounting ratios: anomalies or indicators of firm survival, bankruptcy and fraud? An exploratory study. *Managerial Finance*, 26(11), 5–20.

Amiram, D., Bozanic, Z. & Rouen, E. (2015) Financial statement errors: evidence from the distributional properties of financial statement numbers. *Review of Accounting Studies*, 20(4), 1540–1593.

Andon, P., Free, C. & Scard, B. (2015) Pathways to accountant fraud: Australian evidence and analysis. *Accounting Research Journal*, 28(1), 10–44.

Bao, Y., Ke, B., Li, B., Yu, Y.J. & Zhang, J. (2020) Detecting accounting fraud in publicly traded U.S. firms using a machine learning approach. *Journal of Accounting Research*, 58(1), 199–235.

Beneish, M.D. (1997) Detecting GAAP violation: implications for assessing earnings management among firms with extreme financial performance. *Journal of Accounting and Public Policy*, 16(3), 271–309.

Beneish, M.D. (1999) The detection of earnings manipulation. *Financial Analysts Journal*, 55(5), 24–36.

Beneish, M.D. & Vorst, P. (2022) The cost of fraud prediction errors. *The Accounting Review*, 97(6), 91–121.

Bhattacharya, S., Xu, D. & Kumar, K. (2011) An ANN-based auditor decision support system using Benford's law. *Decision Support Systems*, 50(3), 576–584.

Boulter, T., Mukherjee, A. & Bhattacharya, S. (2013) Motivation for occupational fraud: an analysis of the "fraud triangle" using economic logic. *The International Journal of Interdisciplinary Organizational Studies*, 7(1), 47–57.

Brazel, J.F., Jones, K.L., Thayer, J. & Warne, R.C. (2015) Understanding investor perceptions of financial statement fraud and their use of red flags: evidence from the field. *Review of Accounting Studies*, 20(4), 1373–1406.

Brazel, J.F., Jones, K.L. & Zimbelman, M.F. (2009) Using nonfinancial measures to assess fraud risk. *Journal of Accounting Research*, 47(5), 1135–1166.

Busta, B. & Weinberg, R. (1998) Using Benford's law and neural networks as a review procedure. *Managerial Auditing Journal*, 13(6), 356–366.

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

Chakrabarty, B., Moulton, P.C. & Pugachev, L. (2022) *Catch me if you can: in search of accuracy, scope, and ease of fraud prediction*. Working paper. Available from: https://ssrn.com/abstract=3352667 [Accessed 2nd May 2023].

Cho, W.K.T. & Gaines, B.J. (2007) Breaking the (Benford) law: statistical fraud detection in campaign finance. *The American Statistician*, 61(3), 218–223.

Cohen, J., Ding, Y., Lesage, C. & Stolowy, H. (2011) Corporate fraud and managers' behavior: evidence from the press. *Journal of Business Ethics*, 95, 271–315.

Cressey, D. (1953) *Other people's money: a study in the social psychology of embezzlement*. Glencoe, IL: Free Press.

Davis, J.S. & Pesch, H.L. (2013) Fraud dynamics and controls in organizations. *Accounting, Organizations and Society*, 38(6), 469–483.

Dechow, P.M., Ge, W., Larson, C.R. & Sloan, R.G. (2011) Predicting material accounting misstatements. *Contemporary Accounting Research*, 28(1), 17–82.

Dorminey, J., Fleming, A.S., Kranacher, M.-J. & Riley, R.A., Jr. (2012) The evolution of fraud theory. *Issues in Accounting Education*, 27(2), 555–579.

Dunstan, K. & Gepp, A. (2018) Guest editorial. *Pacific Accounting Review*, 30(2), 130–134.

EY. (2016) *14th Global fraud survey*. Reportno. Report Number|, Date. Place Published|: Institution|.

Fastow, A. (2016) Enron case study. In: *The 15th fraud and cyber crime symposium*. Gold Coast, Qld: Queensland Police Service.

Free, C. (2015) Looking through the fraud triangle: a review and call for new directions. *Meditari Accountancy Research*, 23(2), 175–196.

Free, C., Macintosh, N. & Stein, M. (2007) Management controls: the organizational fraud triangle of leadership, culture and control in Enron. *Ivey Business Journal*, 71, 1–5.

Free, C. & Murphy, P.R. (2015) The ties that bind: the decision to co-offend in fraud. *Contemporary Accounting Research*, 32(1), 18–54.

Gepp, A., Kumar, K. & Bhattacharya, S. (2021) Lifting the numbers game: identifying key input variables and a best-performing model to detect financial statement fraud. *Accounting & Finance*, 61(3), 4601–4638.

Gepp, A., Linnenluecke, M.K., O'Neill, T.J. & Smith, T. (2018) Big data techniques in auditing research and practice: current trends and future opportunities. *Journal of Accounting Literature*, 40, 102–115.

Gillett, P.R. & Uddin, N. (2005) CFO intentions of fraudulent financial reporting. *Auditing: A Journal of Practice & Theory*, 24(1), 55–75.
Goodman, W. (2016) The promises and pitfalls of Benford's law. *Significance*, 13(3), 38–41.
Griffin, J., Kruger, S. & Maturana, G. (2016) Do personal ethics influence corporate ethics? In: *CARE conference: perspectives on fraud*. Leesburg, VA: Proceedings of the National Academy of Sciences (PNAS). Available from: https://ssrn.com/abstract=2745062; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2745062 [Accessed 2nd May 2023].
Guyon, I. & Elisseeff, A. (2003) An introduction to variable and feature selection. *Journal of Machine Learning Research*, 3, 1157–1182.
Hobson, J., Mayew, W. & Venkatachalam, M. (2011) Analyzing speech to detect financial misreporting. *Journal of Accounting Research*, 50(2), 349–392.
Humpherys, S.L., Moffitt, K.C., Burns, M.B., Burgoon, J.K. & Felix, W.F. (2011) Identification of fraudulent financial statements using linguistic credibility analysis. *Decision Support Systems*, 50(3), 585–594.
Kassem, R. & Higson, A. (2012) The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Sciences*, 3(3), 191–195.
Krambia-Kapardis, M. (2001) *Enhancing the auditor's fraud detection ability: an interdisciplinary approach*. New York: Peter Lang.
Krambia-Kapardis, M. (2015) Auditors and fraud detection: an elusive role? In: Rider, B. (Ed.) *Research handbook on international financial crime*. Cheltenham, Glos, UK; Massachusetts: Edward Elgar Publishing, pp. 612–624.
Krambia-Kapardis, M. (2016) *Corporate fraud and corruption: a holistic approach to preventing financial crises*. New York: Palgrave Macmillan US.
Krambia-Kapardis, M. (2022) Editorial. *Journal of Financial Crime*, 29(2), 409–412.
Kranacher, M.-J., Riley, R. & Wells, J.T. (2011) *Forensic accounting and fraud examination*. Hoboken, NJ: John Wiley.
Kumar, K., Bhattacharya, S. & Hicks, R. (2018) Employee perceptions of organization culture with respect to fraud – where to look and what to look for. *Pacific Accounting Review*, 30(2), 187–198.
Lou, Y.-I. & Wang, M.-L. (2009) Fraud risk factor of the fraud triangle assessing the likelihood of fraudulent financial reporting. *Journal of Business & Economics Research*, 7(2), 61–78.
Morales, J., Gendron, Y. & Guénin-Paracini, H. (2014) The construction of the risky individual and vigilant organization: a genealogy of the fraud triangle. *Accounting, Organizations and Society*, 39(3), 170–194.
Murphy, P.R. (2012) Attitude, Machiavellianism and the rationalization of misreporting. *Accounting, Organizations and Society*, 37(4), 242–259.
Murphy, P.R. & Free, C. (2016) Broadening the fraud triangle: instrumental climate and fraud. *Behavioral Research in Accounting*, 28(1), 41–56.
Ndofor, H.A., Wesley, C. & Priem, R.L. (2015) Providing CEOs with opportunities to cheat: the effects of complexity-based information asymmetries on financial reporting fraud. *Journal of Management*, 41(6), 1774–1797.
Nigrini, M.J. (2017) Audit sampling using Benford's law: a review of the literature with some new perspectives. *Journal of Emerging Technologies in Accounting*, 14(2), 29–46.
Perols, J.L. & Lougee, B.A. (2011) The relation between earnings management and financial statement fraud. *Advances in Accounting*, 27(1), 39–53.
Rad, M., Amiri, A., Ranjbar, M.H. & Salari, H. (2021) Predictability of financial statements fraud-risk using Benford's law. *Cogent Economics & Finance*, 9(1), 1889756.
Ramamoorti, S. (2008) The psychology and sociology of fraud: integrating the behavioral sciences component into fraud and forensic accounting curricula. *Issues in Accounting Education*, 23(4), 521–533.
Rezaee, Z. & Riley, R. (2010) *Financial statement fraud: prevention and detection*. Hoboken, NJ: Wiley.
Shafer, W.E., Simmons, R.S. & Yip, R.W.Y. (2016) Social responsibility, professional commitment and tax fraud. *Accounting, Auditing and Accountability Journal*, 29(1), 111–134.
Shahana, T., Lavanya, V. & Bhat, A.R. (2023) State of the art in financial statement fraud detection: a systematic review. *Technological Forecasting and Social Change*, 192(122527), 122527.
Shannon, C.E. (1948) A mathematical theory of communication. *Bell System Technical Journal*, 27(3), 379–423.
Silver, S.E., Fleming, A.S. & Riley, R.A., Jr. (2008) Preventing and detecting collusive management fraud. *The CPA Journal*, 78(10), 46–48.
Skousen, C., Smith, K. & Wright, C. (2009) Detecting and predicting financial statement fraud: the effectiveness of the fraud triangle and SAS No. 99. *Advances in Financial Economics*, 13, 53–81.
Skousen, C. & Wright, C. (2008) Contemporaneous risk factors and the prediction of financial statement fraud. *Journal of Forensic Accounting*, IX, 37–62.
Stambaugh, C., Tipgos, M.A., Carpenter, F. & Smith, M. (2012) Using Benford analysis to detect fraud. *Internal Auditing*, 27(3), 24–29.

Trompeter, G.M., Carpenter, T.D., Desai, N., Jones, K.L. & Riley, R.A., Jr. (2013) A synthesis of fraud-related research. *Auditing: A Journal of Practice & Theory*, 32(1), 287–321.

Wolfe, D.T. & Hermanson, D.R. (2004) The fraud diamond: considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.

Xu, X., Xiong, F. & An, Z. (2022) Using machine learning to predict corporate fraud: evidence based on the GONE framework. *Journal of Business Ethics*, 186, 137–158. Available from: https://doi.org/10.1007/s10551-022-05120-2 [Accessed 2nd May 2023].

How to cite this article: Gepp, A., Kumar, K. & Bhattacharya, S. (2023) Taking the hunch out of the crunch: A framework to improve variable selection in models to detect financial statement fraud. *Accounting & Finance*, 00, 1–20. Available from: https://doi.org/10.1111/acfi.13192