Security Journal
https://doi.org/10.1057/s41284-023-00402-4

ORIGINAL ARTICLE

What really works in preventing fraud against organisations and do decision-makers really need to know?

Mark Button[1] · **Branislav Hock**[1] · **David Shepherd**[1] · **Paul M. Gilmour**[1]

Accepted: 4 September 2023

Abstract

An evidence base of what works using high-quality evaluations in tackling societal problems has become the norm in many spheres, including tackling traditional crime. Yet, as we show in the example of fraud faced by organisations, high-quality evaluations are not always possible, or even necessary for tackling problems effectively. Drawing on a review of over 400 research studies exploring the prevention of fraud, this paper finds a paucity of studies meeting the highest quality of standards of evaluation using the Maryland Scale. This is largely because of the barriers to implementing the Maryland Scale, given the challenges of measuring fraud, rather than because of a low quality of research per se. In the absence of high-quality evaluations, this paper uses a novel alternative to the Maryland scale to identify a range of effective tools that organisations can use to prevent fraud. Finally, the paper provides practical and theoretical reflections upon a broader problem of how and to what extent scientific evaluations of high-quality evidence are necessary in combating fraud effectively.

Keywords Fraud prevention · Fraud measurement · Business crime · Maryland scale of evaluation

✉ Mark Button
mark.button@port.ac.uk

Branislav Hock
branislav.hock@port.ac.uk

David Shepherd
david.shepherd@port.ac.uk

Paul M. Gilmour
paul.gilmour@port.ac.uk

[1] Centre for Cybercrime and Economic Crime, University of Portsmouth, Portsmouth PO1 2HY, UK

Published online: 11 October 2023

Introduction

A patient with severe stomach pains visiting a doctor would expect tests to determine the causes of their illness and an effective treatment plan grounded in scientific evaluation. This expectation of scientific evaluation has been largely present in crime prevention. The police in many countries have been expected to engage in 'evidence based policing', ideally, using randomised control research trials to determine effective crime reduction strategies (Sherman 2013; White and Krislov 1977; Zimring 1976). Moreover, private organisations have been under increasing pressure to introduce effective preventative measures based on artificial intelligence and machine learning to prevent various forms of economic crime (Bank of England and FCA 2019; Canhoto 2020). Yet, when formulating strategies to tackle the escalating fraud problem, neither the police nor private sector organisations will find much high-quality evidence of what works in tackling fraud (Prenzler 2020). Consequently, anyone considering strategies to counter the growing fraud epidemic will often be limited to 'faith-based' approaches learnt in professional training courses and textbooks due to the absence of high-quality evidence that they actually work.

This article demonstrates a lack of quality studies illustrating what works in combating fraud and confirms a study by Prenzler (2020). Moreover, due to difficulties associated with fraud measurement (Tunley 2011, pp. 192–193) and the complex and hidden nature of fraud (Button and Gee 2013; Gilmour 2021), evidence-based policing approaches have serious limitations in relation to fraud (Sherman et al. 2002). The question then arises: to what extent does scientific evaluation evidence of existing fraud prevention initiatives provide evidence they work? Furthermore, if there is a lack of evidence, is it necessary to understand to a high degree of certainty whether counter-fraud initiatives and measures work? These are the central questions this paper seeks to explore. In doing so, it will also seek to show the range of tools that can be used by organisations to combat fraud with evidence of their effectiveness from the limited literature available.

The remainder of the article is structured as follows. The article will first explore key methodological approaches to evaluating whether crime initiatives work and illustrate methodological challenges associated with measuring and evaluating the fraud problem. The methods of this paper will then be outlined before revealing the limited base of literature that evidences what works and what does not in combating fraud by organisations. The paper will then conclude with a discussion considering whether and how scientific evaluations are necessary in combating fraud. Whilst this article will primarily discuss the problem of determining what works in the context of organisations combating fraud, the findings are applicable more generally to other forms of economic crime prevention strategies.

Scientific crime reduction analysis and the fraud problem

The importance of understanding what works in crime prevention in the USA stimulated a programme of scholarly activity which culminated in the application of a medical model of scientific evaluation to crime prevention (Sherman et al. 1997, 1998). The most widely used quality evaluation scale in the criminal justice context is the Maryland Scale of Scientific Methods (Sherman et al. 1998; see also Hayhurst et al., 2015). The Maryland scale uses five levels with each additional level becoming more robust, which builds upon medical approaches to determine if treatments or drugs work:

Level 1 Correlation between a crime prevention programme and a measure of crime or crime risk factors at a single point in time.

Level 2 Temporal sequence between the programme and the crime or risk outcome clearly observed, or the presence of a comparison group without demonstrated comparability to the treatment group.

Level 3 A comparison between two or more comparable units of analysis, one with and one without the programme.

Level 4 Comparison between multiple units with and without the programme, controlling for other factors, or using comparison units that evidence only minor differences.

Level 5 Random assignment and analysis of comparable units to programme and comparison groups (Sherman et al. 1998, pp. 4–5).

Sherman et al. (1997, 1998) were able to provide a comprehensive analysis of hundreds of projects using this Maryland framework to determine what works in preventing crime and what does not. This scientific analysis has fundamentally influenced the approach many governments and law enforcement agencies take in their effort to develop effective crime reduction strategies (Sherman et al. 2002; College of Policing, n.d.).

Although there is extensive evidence of the growth of fraud and other economic crimes in many countries (Button et al. 2022; Levi and Smith 2021; Kemp et al. 2021), the literature of what works in crime prevention, however, has largely ignored fraud.[1] Fig. 1 below illustrates the growth in England and Wales of fraud and computer misuse set against traditional crimes *against individuals* using the Crime

[1] For the purposes of this article, the notion of fraud is defined broadly as "the intention to dishonestly deceive a person or legal entity in order to make a financial or economic gain for the offender or another, or to cause a financial or economic loss to the person or legal entity, such that there is a prima facie case for criminal, civil or regulatory justice" (Button et al. 2022, p. 34).

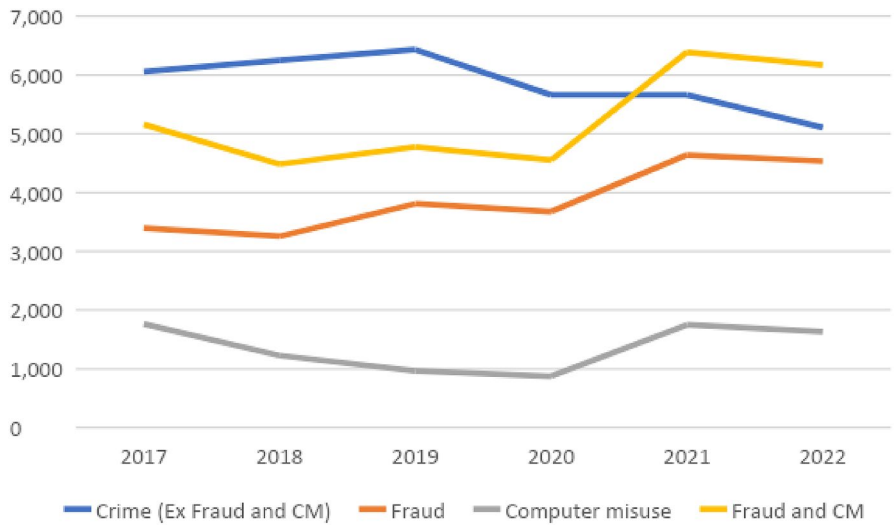

Fig. 1 Fraud, Crime and Computer Misuse in England and Wales 2017–2022. *Source* ONS (2023)

Survey for England and Wales. It shows how fraud almost accounts for the same number of all traditional crimes (burglary, theft etc.) and that, when computer misuse is added (many of which are attempted frauds), it exceeds traditional crime.

There are several challenges with these statistics. First, the CSEW data only cover individual victims and not organisations. The Government in the UK does commission a regular commercial victimisation survey, but this is only at the establishment level and does not cover all business sectors, as is the case with the new Home Office Economic Crime Survey (Home Office 2022, 2023). Thus, data on organisational fraud victimisation are limited. Second, it is important to note fraud by its very nature is a hidden crime: there is not usually 'a body' to illustrate a crime has occurred (Tunley 2011). This is especially true in an organisational context (Shepherd and Button 2019). Hidden in the transactions of many organisations will be frauds which remain undetected: exaggerated expense claims by staff, invoices paid for services which have not all been delivered, payments for overtime not worked, purchases of additional equipment that are for staff, not the organisation etc. This is just a snapshot, but the important issue to note is that uncovering these frauds requires counter-fraud activity and the quality and extent of that activity varies between organisations (Button and Gee 2013). Thus, the detection of fraud in an organisation reflects the quality, extent and effectiveness of its counter-fraud activities.

Third, an organisation might relabel fraud as something else. Consider invoice fraud and a supplier which has submitted the same invoice twice. This could have been deliberate as the supplier worked out the organisation's systems and those systems did not detect the fraud, or it could have been a genuine mistake. The transaction could be labelled as fraud if there was evidence of deliberate intent to submit twice, or it could be equally labelled an error. Thus, there are often opportunities

for organisations to relabel such incidents as something other than fraud, for example, an error, contractual breach, or bad debt. Therefore, detected or reported levels of fraud within an organisation are largely flawed measures, with the exception of banking fraud. The banking and credit fraud statistics are one of the few areas of fraud statistics that are reasonably accurate because customers tend to notice unusual transactions against their credit cards and bank accounts and report them (Button et al. 2009). The banks are also effective at detecting frauds against themselves by customers (Delamaire, et al. 2009).

The challenges with measuring fraud have led to innovative ways to overcome the problem. One approach is a fraud loss measurement exercise (Button et al. 2015a, 2015b). This works for homogenous groups of transactions such as social security claims, insurance claims, payroll and procurement. Under this approach from the total population of transactions a sample is taken; the type of which may vary according to the nature and size of the population. These transactions are then *all* investigated to determine whether they are frauds, errors or legitimate. The results of the investigations can then be used using appropriate statistical methods to estimate the levels of fraud and loss in the total population. Such methods have been largely used in the public sector and vary in their level of statistical ranges and levels of confidence. For example, the UK the Department for Work and Pensions uses such approaches to measure fraud in social security. Consider, the most recent measurements of fraud associated with the following benefits (DWP 2022):

- Universal credit 13% fraud £5.9 billion value.
- Housing benefit 3.3% fraud £540 million value.
- Employment Support Allowance 2% £250 million.

Unfortunately, fraud loss measurement and similar approaches can be time consuming and costly. The results can also be politically unpalatable (Button et al. 2015b). But they produce much more accurate levels of fraud loss than approaches based on fraud reporting. Fraud loss measurement could allow for a more accurate measurement of what actually works and what does not in combating fraud by organisations.

Studies on the prevention of fraud have also been rare, as Prenzler (2020, pp. 83–84) has noted:

> Given the size and growth of the fraud problem, it would be reasonable to expect a large number of well-documented intervention studies aimed at demonstrating successful anti-fraud strategies. However, this does not appear to be the case. The fraud literature has been characterised by descriptive statistics of the dimensions of the problem, and analyses of victim and offender characteristics and opportunity factors, with very little on prevention, especially in terms of applied projects.

Indeed, Prenzler (2020) in his extensive review found only 24 evaluation reports covering 19 projects and many of these studies related to very narrow areas of fraud such as welfare fraud and card fraud. A further illustration of this dearth of literature can be seen by visiting the Situational Crime Prevention Evaluation Database at the renowned ASU Center for Problem-Oriented Policing website (ASU, n.d.). A search

for ‘fraud’ on the website produces a list of only 7 studies, focussed upon card fraud and welfare fraud, compared to 45 for ‘burglary’. Furthermore, consider the US National Institute of Justice Crime Solutions website, another repository of what works in crime prevention, which does not even have a fraud listing (US National Institute of Justice Crime Solutions, n.d.).

By comparison, any search of Google Scholar or Scopus reveals dozens of studies evaluating fraud prevention initiatives, with many drawn from beyond criminological studies, such as management studies, psychology, computer science and mathematics (Button and Shepherd 2023). However, as this paper will show, many of these studies use methods of evaluation which do not even meet Level 1 of the Maryland scale. Before exploring some of these studies, we first outline the methodological approach.

Methods

To investigate how and to what extent scientific evaluation evidences whether existing fraud prevention initiatives and measures work, the authors undertook a structured literature review seeking high-quality outputs from academic and grey literature sources. The principal tool for literature search was Scopus using a variety of search terms around ‘fraud and prevention’. The search also included studies that have evidence on factors that influence levels of fraud. Scopus does not cover all literature and searches were also supplemented with Google Scholar and Google. The authors also targeted specific organisations who were known to produce reports in this area and any reports evaluating fraud prevention initiatives were noted. The focus upon quality outputs from academic and grey literature meant outputs from outlets like newspapers and magazines were excluded. All these outputs for fraud were added to an Excel sheet for assessment. In total, 1666 fraud studies were located, of which 488 covered some form of evidence exploring a disruptive tool or strategy targeting fraud.

The literature review focussed on two key aspects. The first one was the quality of evidence presented in the literature and the second was concerned with how a wide range of tools are useful in preventing, detecting and disrupting fraud.

The quality of evidence presented in the literature

The essence of the Maryland scale, the highest quality indicators of effectiveness, is a test of an intervention in the real world, hence, not an experiment with students or other participants, assessing the impact before and after. Such an exercise would meet Level 1 of the scale and as the scale progresses more rigour is applied such as temporal assessments, control groups through to highest ranking random assignment of comparative groups for intervention with control groups, which take into account other factors which may have influenced the results.

Studies using methodologies ranking on the Maryland scale, however, were rare. Indeed, for fraud-related tools, the researchers only found 15 studies, plus one report

detailing an overview of several studies that met or were equivalent to the Maryland scale (Bilcher and Clarke 1996; Blais & Bacher 2007; Cabinet Office 2020; Challenger 1996; Cross 2016; Detert et al. 2007; Fellner et al. 2013; Greenberg 1990; Kim et al. 2019; Knutsson & Kuhlhorn 1997; Masuda 1993; Schwartz and Orleans 1967; Webb 1996). Some of these studies were outdated and not relevant to the current nature of fraud against organisations, such as the Cross (2016) study focussed upon individual victims.

In conducting this review, the authors identified a wide range of tools discussed in the research as useful in preventing, detecting and disrupting fraud. However, the quality of evidence that they actually work is much weaker and most do not use a methodology that would meet the thresholds of the Maryland scale. Evidence included,

- Views of practitioners based upon their past experience.
- Literature based studies.
- Structured literature based studies.
- Surveys of organisations with their levels of fraud and controls in place that uses statistical analysis to identify the most effective tools that influence fraud levels.
- Surveys of practitioners asking them to rank effectiveness of tools.
- Interviews with experts/fraudsters to identify what works.
- Experiments (usually with students) which test whether certain controls work or not.
- The use of an existing dataset (such as credit card transactions, with known fraud and correct) which is then tested to produce tools/algorithms to detect/prevent fraud.

Much of this evidence is weak compared to Maryland ranking studies, but that does not necessarily mean the strategies do not work. The inability to apply Maryland criteria to many of these studies led the authors to develop a more pragmatic approach and rated tools according to the following criteria:

> No Evidence: No clear quality evidence suggests a tool has an impact on fraud.
> Unclassified: where there is both positive and negative evidence a tool/strategy may work and it is therefore difficult to determine if it works.
> Promising: at least two studies of appropriate quality from different researchers rooted in primary research showing the intervention works.
> Very Promising: at least three studies from different authors of appropriate quality rooted in primary research showing the intervention works, with at least one of those studies ranked on the Maryland Scale.

Scientific evidence of whether fraud prevention initiatives and measures work

Whilst the vast bulk of literature assessing tools to counter fraud does not meet the Maryland scale threshold, there were some that show the effectiveness of counter-fraud tools. One of the higher quality approaches to assessment outside the

Maryland scale are studies that seek evidence of fraud victimisation in a sample of organisations, identify the different fraud prevention strategies the organisation has in place and then undertake statistical analysis to determine which tools have greater impact based upon a sample of different organisations—the ACFE Report to the Nation regularly does this (see ACFE 2022). However, as correlation does not mean causation, even these stronger positivist studies serve to illustrate the weak base of evidence in the literature. In the following sections, we present an analysis of how a wide range of tools are useful in preventing, detecting and disrupting fraud.

Very promising tools and strategies with very good evidence that they work

These were tools and strategies with at least three studies illustrating they work with at least one ranked on the Maryland scale. The first type of set of tools that can be considered as fitting this category is 'appropriate controls/procedures; situational opportunity reducing measures'. This is a broad category and it is important to note many articles and reports do not define what they mean by controls or use very narrow approaches. For the purpose of this article, we have taken a wider interpretation to consider any control implemented to reduce potential opportunities for fraud both for internal and external frauds. The essence of this broad body of evidence is that there are a variety of studies that show through various methodologies that when controls are implemented fraud can be reduced. This can range from controls to reduce telephone fraud (Bichler and Clarke 1996) to tackling refund fraud (Challinger 1996) through to combatting staff fraud through classic 'internal controls' such as segregation of duties and multiple signatories (ACFE 2020).

There are dozens of studies in a variety of contexts which advocate, model or actually assess the benefits of using various *data-analytical techniques* to detect, deter and prevent various types of fraud (Cabinet Office 2020; Kim et al 2019). Data-analytics in the broadest sense can be divided into data matching—the comparison of different datasets to detect potential fraud (e.g. list of dead people versus people claiming pensions); data sharing—linked to data matching is data sharing, where organisations who legally can work together to share data for the purposes of the former and data mining—the use of data to identify anomalies which suggest fraud. Such techniques vary in complexity from the simple analysis of transactions to identify outliers (such as Benford's law), to sophisticated approaches looking at multiple pieces of data such as prior spending behaviours or the location of transaction. Some use complex algorithms and machine learning to refine their effectiveness. For example, many online retailers will use such methods to identify and reject high risk sales transactions.

There is a great deal of research that covers this area. The bulk of which is related to data-mining type approaches. Many of the studies are proposals for approaches to better detect fraud that are usually built upon past datasets of transactions. They often use complex maths to develop algorithms which they advocate. There are less studies that look at the implementation of such measures and identify the impact. The evidence from the Cabinet Office (2020) on data matching and Kim et al. (2019) on data-mining approaches in a bank illustrate very good evidence. There are clearly

many other studies which identify the benefits of such approaches. This clearly is a tool that if directed at the right type of fraud with the appropriate data-analytics works. There are, nevertheless, many different versions and the complexity of them is such that further research is warranted to distinguish the full-range of data-analytical techniques and determine each of their effectiveness in different contexts.

Messaging or nudging rooted in behavioural insights **methodologies** have been shown to work in a wide range of areas beyond fraud, but there is also evidence from fraud too. The studies in this category have shown that sending appropriately worded messages and designing processes to maximise compliance (such as where declarations are signed) can reduce levels of fraud (Ariely 2012). It is, however, important to create the right message as the study by John and Blume (2018) noted, crafted incorrectly, it can be counter-productive.

There is also clear evidence that targeted *anti-fraud campaigns/targeted initiatives* can also impact fraud. Blais and Bacher (2007) illustrate this via a campaign to reduce insurance fraud in Canada and Cross (2006) in targeting known victims, which although based upon individuals, has potential for organisations too.

Appropriate managerial supervision was a strategy that fitted this category. Detert et al. (2007) studying a chain of restaurants found the amount of supervision had an impact on fraud, with less supervision leading to more and that abusive supervision could also lead to more fraud too. Other studies using weaker methodologies have also supported this as an effective tool (ACFE 2020; N'Guilla Sow et al. 2018).

Tone from the top is frequently mentioned as a tool to reduce fraud and other negative behaviours. Here again there is some good evidence that this works. The classic Greenberg (1990) study showed how a more respectful and informative tone when implementing a negative thing such as a pay cut had an impact on reducing levels of staff theft. The study by Detert et al (2007) also illustrated how a negative tone from management could lead to more fraud among some other studies (Greuning and Brajovic 2020; Leighton-Daly 2017).

Another strategy with good evidence of having an impact on fraud is *fraud awareness training for staff*. Masuda (1997) found that a targeted strategy in a retail chain, which included, staff training in fraud led to greater detection of fraud and significant reduction in losses. There are several other studies that illustrate the effectiveness of using lesser quality methodologies listed in the table above. *Disruption of fraudsters*, such as taking down the websites, also has much promise (Moore and Clayton (2007).

Promising tools and strategies with some evidence they work

The evidence that tools and strategies work now starts to get weaker. Promising are tools and strategies of which there is at least one study suggesting they work from different groups of scholars, but none reach the minimum standards of the Maryland scale.

In the accounting literature, there are a number of studies that look at how to prevent accounting/financial statement frauds. The *governance* of a company and characteristics of an *audit committee* in particular (such as number of independent members) are frequently advocated (ACFE 2020; Krambia-Kapardis and Zopiatis 2010; Mangala and Kumari 2017; Soltani 2014; Williams 2018). These studies link various governance measures through statistical analysis of occurrence of fraud or violations with these structures set against measures in place. Much of the same literature also explores the use of *risk management* as a means to address this type of fraud; although, there is also literature which examines different types and methods of risk management as having varying effectiveness, such as based upon who identifies risks and the nature of how they were identified. For occupational/staff fraud, the ACFE (2020) research also illustrates that the presence of this strategy is linked to lower median losses to fraud.

Internal audit is another important tool for both financial statement frauds and most other types of fraud against an organisation with some evidence of effectiveness (ACFE 2020; Peltier-Rivest 2009; Rae and Subramaniam 2008; Zeng et al. 2020). *Recruitment screening/vetting* of new employees is noted as an important tool for preventing insider frauds. There was evidence from one study, however, that there are limitations to securing enough meaningful data to undertake such assessments effectively (Kühn and Nieman 2017) and not all internal fraudsters have prior blemishes on their character.

Authentication measures such as chip-and-pin and biometric measures for payment security are so ubiquitous, one would expect there to be multiple studies evaluating their effectiveness in reducing fraud, but there were very few. Some related to the UK refer to UK Finance statistics, but no publicly available reports were offering quality evidence of impact linked to strategies. There is some evidence of possible displacement to other crimes and methods, but whether the impact of displacement exceeds the benefits has not been determined. Like so many other areas, more research is required.

Fraud measurement or payment recapture audits have been advocated (including by the authors) where organisations sample random selections of similar transactions (applications, procurement payments, payroll etc.), assess them for fraud, then estimate the levels of fraud in the population within confidence intervals, and most importantly then target action at where losses occur. There is evidence such approaches work, but it is not based on evaluations with the rigour of the Maryland scale (Button and Gee 2013; Owens & Jessup 2014). *Hotlines for reporting/whistleblowing* have been placed together, but they could be seen separately as hotlines do not always guarantee anonymity. Given such measures are regularly advocated by counter-fraud professionals, one would again expect extensive evidence they work in reducing fraud. However, the extent to which they expose fraud and their effectiveness in reducing the rate of fraud loss is difficult to determine from the literature, with limited high-quality studies (see for example Latan et al. 2019; Maulida and Bayunitri 2021).

Cyber-awareness training is targeted at cybercrimes, including those that enable fraud. So training that seeks to reduce susceptibility of staff to phishing and social engineering attacks would seem important. There is a small base of literature that

suggests such cyber-awareness training can reduce the frequency of staff falling victim to phishing attacks, which, by implication, would be expected to impact on fraud levels. Examples include companies such as Cofense (2021) which educate employees on phishing, send out simulated phishing attacks and seek to improve behaviours of those at greater risk.

In the enforcement area for organisations, there is also evidence that the *threat of sanctions* or *actual use of sanctions* against staff and customers can reduce levels of fraud, as can increasing the perception of the chances of getting caught. Blais and Bacher (2007) in a study related to insurance fraud (see Table 1) noted reduced claims from customers who were warned of the potential of prosecution. Schwartz and Orleans (1967) in a study related to tax returns found informing citizens of the potential sanctions a month before tax submission produced higher returns than not, although, appealing to their conscience was even more successful. In another study involving over 50,498 members of the public in Austria, an experiment using 6 different compliance messages were sent to 6 groups, some with threats (stressed high detection rate and sanctions if caught), others with social information or moral appeals. The threat produced a small (2%) increase in compliance over the standard reminder, compliance reduced with the social information and moral appeal letters (Fellner et al. 2013).

Surprise audits and *dedicated counter fraud function* are listed as tools because of the ACFE (2020) or similar studies. The ACFE (2020) data have shown these strategies reduce the median losses due to occupational fraud. This is not strong evidence, but again, it is important to reiterate that the lack of evidence is a reflection of the lack of research evaluating them, not necessarily that they do not work.

Resilience/vulnerability assessments could be considered a form of risk management. Based upon a standard of what is perceived to be good practice in countering fraud, an organisation benchmarks itself against that standard, with the implication it will prompt them to address shortcomings. Such an approach has become prominent in tackling food fraud with a variety of assessments (Spink et al. 2019). The principle behind them seems sound, but there is virtually no evidence that they actually lead to a reduction in levels of fraud.

Unclassified tools/strategies

These are tools/strategies where there was some supporting evidence of their effectiveness, but conflicting studies of similar quality found they did not work. This lack of consensus is apparent for *anti-fraud policy, code of conduct, barring contractors, employee assistance programmes* and *external audit*. The latter is a particularly contentious issue, not least over whether it is even the duty of external auditing to find fraud. In a survey of counter-fraud professionals asking them what worked in countering occupational fraud, Tunley et al. (2018) found external audit was the lowest ranked of 18 different tools. In the area of *monitoring websites/darkweb*, there was limited supporting evidence that tools such as web crawlers, which automatically search the internet, could offer some benefits (Sapienza et al. 2018).

Table 1 Examples of very promising interventions which have been evaluated to a high standard

Study	Tool	Fraud context and brief description
Blais and Bacher (2007)	Anti-fraud deterrence campaign and behavioural insights	*Insurance fraud* An experiment in Canada involving 4 insurance companies and 765 participants. Property theft claims randomly assigned to experimental group or control group. Claimants in the experimental group were sent a form by post or email to inform them that the company was concerned about claim padding, was prepared to prosecute fraudsters, remind claimants of sanctions, and point out that it is generally regarded as dishonest; the claimants had to sign and return the form. The control group claims were processed in the companies' normal way. The average claim value of the experimental group was 15% ($300) lower than the control group ($2,470 cf $2,770)
Challinger (1996)	Targeted controls	*Refund fraud in retailing* This study looked at one major retail chain in Australia. Refund fraud was a problem so the group introduced a control where proof of purchase was required to secure a refund. As a consequence, there was a significant reduction in losses to retail fraud
Detert et al. (2007)	Management supervision and style	*Employee theft and fraud in restaurants* This study is based upon 265 restaurants and over 10,000 staff. It used perception surveys and actual losses. Perceptions of managerial style were gauged from the survey (abusive supervision—which is where superiors engage in hostile verbal and non-verbal behaviours towards subordinates and ethical leadership—the promotion and demonstration of appropriate conduct) along with actual company data on levels of supervision in the unit. It found abusive supervision increases fraud loss, less supervision increases fraud loss but ethical leadership has no effect. So they found abusive management and lack of supervision leads to more fraud, ethical leadership is neutral it does not lead to more or less fraud
Greenberg (1990)	Tone from top, management style	*Employee theft* This study explored the impact of a pay cut and the way it is justified. Three comparable manufacturing plants were selected. One was a control with no pay cut. Two received pay cut and one was given an adequate justification from management, the other a lesser response. Rates of staff theft and other negative indicators rose in the plant with the inadequate response compared to the control and adequate response. Although this study is directed at staff theft, the overlaps with staff fraud and the uniqueness of this study warrants inclusion. It shows that if staff experience negative news from the organisation they work for, the tone from the top in conveying that news is very important in reducing potentially negative consequences which might arise from it such as theft and fraud

Table 1 (continued)

Study	Tool	Fraud context and brief description
Kim et al. (2019)	Data-analytics for detection	*Card fraud against banks* This study examined the introduction of a new detection method in a Korean bank which was using a hybrid ensemble of analytical detection methods (decision trees, logistic regressions, and shallow neural networks), which is the industry standard. Tested across 3 months against an alternative deep learning model with multiple layers of neural networks. The deep learning model performed better increasing the percentage of fraudulent cards detected by 6% to 81%
Knutsson and Kuhlhorn (1997)	Targeted controls	*Cheque fraud in Sweden* This study reported on the impact of the introduction of two controls on cheque fraud in Sweden. Following a rise in the crime, two controls were introduced the removal of a bank guarantee and the requirement to produce identity. This led to an 81% reduction in fraud which was sustained for several years afterwards
Masuda (1993)	Targeted controls, including staff fraud awareness training	*Retail fraud* This is a case study of one American retailer selling electrical goods. The company instigated a new counter-fraud programme which involved training of staff, rewarding them if they detected fraud, profiling of shoppers, sanctions against fraudsters among others. The result of the programme was a substantial increase in fraud reports from 47 to 118, but a reduction in losses from $1.1 million to $200 k year to year
Webb (1996)	Targeted controls	*Credit card fraud* This paper looks at credit card fraud between 1990 and1994 in the UK. It looks at the trends, charts the strategies introduced to reduce it and as consequence claims a reduction of 41% in losses 1991–1994. The preventative strategy included, lowering floor limits for authorisation, a hot file of stolen/lost cards and delivering cards by couriers

No evidence

There was also a wide range of tools/strategies found with no supporting evidence that they have an impact on reducing fraud. These included *post recruitment screening, checks on clients, contractors, tests (integrity and system), forensic accountants/investigators within companies, rewards for whistleblowers, red flag monitoring, lie detection technologies for fraud, fraudster registers*. Rewards for whistleblowers are also the only tool on the ACFE (2020) list which has no impact on median fraud losses.

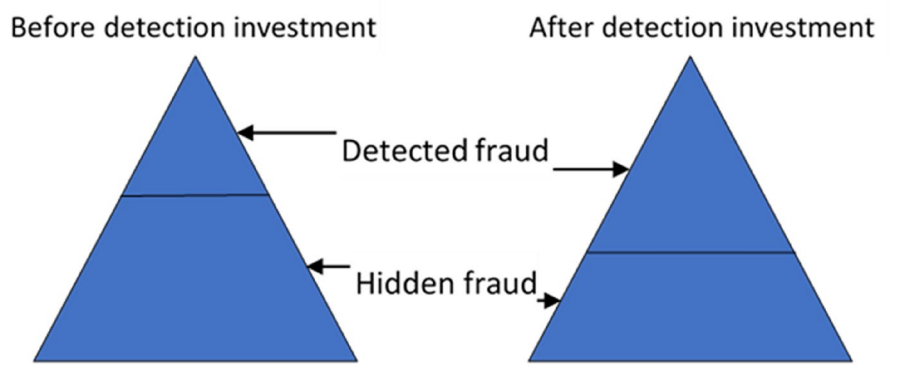

Fig. 2 The increased detection of fraud challenge for measurement

Discussion

This paper raises some important questions about the selection of tools to reduce fraud for organisations and the necessity of quality evidence to prove they work. It is important to remember that the use of the Maryland scale originates from medical studies in which clinical decisions based on medical evidence rely on treatments or interventions working—after all, if they do not work, a patient's condition could deteriorate or, even worse, the patient could die. Whilst some crimes, including frauds, may result in such serious consequences for individual victims, most do not (Button et al. 2014), and the consequences for organisational victims are overwhelmingly financial (Button 2015a). This perhaps leads to the conclusion that the quality of empirical evidence in support of a counter-fraud method is less critical than that required for clinical trials. The lack of evidence is essentially an efficiency problem: if a counter-fraud tool is effective it reduces losses and improves efficiency; if it fails, then time, effort and money is wasted. We also need to consider that, even if the empirical evidence that methods work, doing nothing is not a sensible option for most organisations. Implementing strategies and tools that are commonly used is better than doing nothing.

This article has also shown that whilst there is not a great deal of high-quality empirical evidence, there is mediocre evidence that offers some promise. Multiple studies using different methodologies show some evidence that a range of tools work. There is also isomorphic learning that can be applied from broader situational crime prevention/routine activity theory—which in the opportunity driven fraud sphere offers much inspiration (Smith and Clarke 2012). Reducing opportunities for fraud is ultimately likely to reduce it.

We also have to consider this debate in the tricky context of measuring fraud. As was noted earlier, counting the number of detected frauds is often useless as an accurate measure of fraud rates for organisations. Consider an organisation that purchases a new data-analytics product to combat procurement fraud. Let us imagine they spend £50 million on procurement per year in circa 25,000 transactions. In the

year prior to the adoption of the new analytics tool, they discovered £250,000 of fraud—0.5%. Subsequently, in the first year of use, the tool helps the organisation uncover £750,000 of fraud—1.5%. It would appear that the fraud rate has increased, but in reality the new tool has proved more effective in detecting more hidden fraud. Figure 2 illustrates how in year 2 the organisation has merely revealed a greater amount of hidden procurement fraud.

The only certain way to know if fraud has decreased in procurement would be to conduct a fraud loss measurement exercise before and after an intervention. However, this would add additional expense to the initiative and make evaluation prohibitive for some. Nevertheless in the financial services sector detected data possibly offers more scope and there are other areas such as insurance claims, social security and tax fraud in which the cost of fraud might warrant the investment in more expensive fraud loss measurement.

Even where there is evidence a strategy or tool works, it is also important to be very conscious of context. There is high-quality evidence that data-analytics technologies work in data-rich contexts with high volumes of similar transactions, such as banking and social security payments. Yet, it is likely to be less effective for a contract engineering business with highly volatile sales and heterogeneous transactions. Similarly, there is also a reasonable body of evidence that the audit committee's role in reviewing draft financial statements prevents financial misstatement fraud, but it would have little impact on payment redirection fraud. So even with evidence of strategies that do work we must be careful to consider the context in which they do.

This discussion leads us back to one of the central academic debates on how we come to understand knowledge about the distinction between positivist approaches and constructivist approaches to research. In ascertaining whether things work, proponents of both perspectives will argue their approach is better. Pragmatists will argue there are benefits to both approaches and this is perhaps where we end up in this discussion. Organisations would welcome to have a repository of evidence of the effectiveness of different tools and strategies in varying contexts in order to inform policy and investment decisions using positivist type methodologies. Where the costs and harms of fraud are high, there is clearly a strong case for evaluations that give greater certainty that tools and strategies work. Where there are large sums of public money at stake this also invokes the need for greater certainty. However, the costs and challenges, particularly, in measuring outcomes, make such positivist evaluations often impractical.

In the absence of high-quality evidence, businesses and governments should be pragmatic and use a mix of tools rooted in varying quality and in some occasions have 'faith' they work. There are some contexts and areas, such as when the cost of fraud is very high or when the fraud problem is relatively less complex, which clearly should be a priority to determine what works, evidenced to a very high standard, or at least useful to know. For the private sector, one could argue it is their choice, if they want evidence of what works, fund research to achieve that. However, there has been ample investment by governments in research to explore if crime prevention schemes work which have benefited businesses (Sherman et al. 2002). It is

in the interest of all in society to reduce fraud, so there is a case for more government investment in fraud prevention research too, to help businesses.

Conclusion

This paper has explored the evidence of what works in combating fraud against organisations. It began by illustrating the growing challenge of fraud and the different problems that exist in measuring it. There were very few studies meeting the highest standards of evaluation, but there were many more studies using lesser quality methodologies and identified what works using the categories 'very promising', 'promising', 'unclassified' and 'no evidence'. Furthermore, the article explored whether higher quality evidence of effectiveness is necessary and concluded that additional investment in research featuring high-quality evidence should be a priority to pursue in some areas, especially when the cost of fraud is very high or when the fraud problem is relatively less complex. However, in the absence of such evidence, additional investments are not always appropriate and decision-makers should use lesser quality evidence with some 'faith' they might work.

Declarations

Conflict of interest There are no conflicts of interest to declare.

Human and animal rights This paper involved no research with human or animal participants.

References

ACFE. 2022. Report to the Nations. https://legacy.acfe.com/report-to-the-nations/2022/. Accessed 27 Jan 2023.

ACFE. 2020. Report to the Nations. https://www.acfe.com/report-to-the-nations/2020/. Accessed 27 Jan 2023.

Ariely, D. 2012. *The honest truth about dishonesty*. New York: HarperCollins.

ASU Center for Problem-Oriented Policing. https://popcenter.asu.edu/content/situational-crime-prevention-database-home.

Bank of England and FCA. 2019. Machine Learning in UK Financial Services. https://www.bankofengland.co.uk/report/2019/machine-learning-in-uk-financial-services. Accessed 27 Jan 2023.

Bichler, G., and R. Clarke. 1996. Eliminating pay phone toll fraud at the port authority bus terminal in Manhattan. *Crime Prevention Studies* 6: 93–115.

Blais, E., and J. Bacher. 2007. Situational deterrence and claim padding: Results from a randomized field experiment. *Journal of Experimental Criminology* 3 (4): 337–352. https://doi.org/10.1007/s11292-007-9043-z.

Button, M., D. Blackbourn, C. Lewis, and D. Shepherd. 2015a. Uncovering the hidden cost of staff fraud: An assessment of 45 cases in the UK. *Journal of Financial Crime* 22 (2): 170–183. https://doi.org/10.1108/JFC-11-2013-0070.

Button, M., and J. Gee. 2013. *Countering fraud for competitive advantage*. New York: Wiley.

Button, M., C. Lewis, and J. Tapley. 2014. Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal* 27 (1): 36–54.

Button, M., C. Lewis, and J. Tapley. 2009. A better deal for fraud victims: Research into victims' needs and experiences. https://pure.port.ac.uk/ws/portalfiles/portal/1924328/NFA_Report_1_15.12.09.pdf. Accessed 27 Jan 2023.

Button, M., C. Lewis, D. Shepherd, and G. Brooks. 2015b. Fraud in overseas aid and the challenge of measurement. *Journal of Financial Crime* 22 (2): 184–198. https://doi.org/10.1108/JFC-02-2014-0006.

Button, M., B. Hock, and D. Shepherd. 2022. *Economic crime: From conception to response*. Abingdon: Routledge.

Button, M., and D. Shepherd. 2023. The case for economic criminology. *Journal of Economic Criminology*. https://doi.org/10.1016/j.jeconc.2023.100015.

Cabinet Office. 2012. Applying behavioural insights to reduce fraud, error and debt. https://www.bi.team/wp-content/uploads/2015/07/BIT_FraudErrorDebt_accessible.pdfs. Accessed 27 Jan 2023

Cabinet Office. 2020. National Fraud Initiative Report July 2020. https://www.gov.uk/government/publications/national-fraud-initiative-reports. Accessed 27 Jan 2023.

Canhoto, A.I. 2020. Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. *Journal of Business Research*. https://doi.org/10.1016/j.jbusres.2020.10.012.

Challinger, D. 1996. Refund fraud in retail stores. *Security Journal* 7 (1): 27–35.

Cofense. 2021. Annual State of Phishing Report 2021. https://cofense.com/. Accessed 27 Jan 2023.

College of Policing. n.d. Evidence Based Policing. https://www.college.police.uk/research/evidence-based-policing-EBP.

Cross, C. 2016. Using financial intelligence to target online fraud victimisation: Applying a tertiary prevention perspective. *Criminal Justice Studies* 29 (2): 125–142. https://doi.org/10.1080/1478601X.2016.1170278.

Delamaire, L., H. Abdou, and J. Pointon. 2009. Credit card fraud and detection techniques: A review. *Banks and Bank Systems* 4 (2): 57–68.

Detert, J., L. Trevino, E. Burris, and M. Andiappan. 2007. Managerial modes of influence and counterproductivity in organizations: A longitudinal business-unit-level investigation. *Journal of Applied Psychology* 94: 993–1005. https://doi.org/10.1037/0021-9010.92.4.993.

DWP. 2022a. Fraud and error in the benefit system Financial Year Ending (FYE) 2022. https://www.gov.uk/government/statistics/fraud-and-error-in-the-benefit-system-financial-year-2021-to-2022-estimates/fraud-and-error-in-the-benefit-system-financial-year-ending-fye-2022. Accessed 27 Jan 2023.

Fellner, G., R. Sausgruber, and C. Traxler. 2013. Testing enforcement strategies in the field: Threat, moral appeal and social information. *Journal of the European Economic Association* 11 (3): 634–660.

Gilmour, P.M. 2021. Exploring the barriers to policing financial crime in England and Wales. *Policing* 15 (2): 1507–1521. https://doi.org/10.1093/police/paaa081.

Greenberg, J. 1990. Employee theft as a reaction to underpayment inequity: The hidden cost of pay cuts. *Journal of Applied Psychology* 75 (5): 561–568.

Greuning, H., and B.S. Brajovic. 2020. Analyzing banking risk: A framework for assessing corporate governance and risk management. World Bank Group

Home Office. 2023. Economic Crime Survey 2020. https://www.gov.uk/government/publications/economic-crime-survey-2020. Accessed 4 May 2023.

Home Office. 2022 Crime against businesses: findings from the 2021 Commercial Victimisation Survey. https://www.gov.uk/government/statistics/crime-against-businesses-findings-from-the-year-ending-march-2021-commercial-victimisation-survey/crime-against-businesses-findings-from-the-2021-commercial-victimisation-survey.

Kemp, S., D. Buil-Gil, A. Moneva, F. Miró-Llinares, and N. Díaz-Castaño. 2021. Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice* 37 (4): 480–501.

John, P., and T. Blume. 2018. How best to nudge taxpayers? The impact of message simplification and descriptive social norms on payment rates in a central London local authority. *Journal of Behavioral Public Administration* 1 (1): 1–11.

Kim, E., et al. 2019. Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning. *Expert Systems with Applications* 128: 214–224. https://doi.org/10.1016/j.eswa.2019.03.042.

Knutsson, J., and E. Kuhlhorn. 1997. Macro-measures against crime: The example of check forgeries. In *Situational crime prevention: Successful case studies*, ed. R. Clarke, 113–121. Guilderland: Harrow and Heston.

Krambia-Kapardis, M., and A. Zopiatis. 2010. Investigating incidents of fraud in small economies: The case for cyprus. *Journal of Financial Crime* 17 (2): 195–209. https://doi.org/10.1108/13590791011033890.

Kühn, S., and A. Nieman. 2017. Can security vetting be extended to include the detection of financial misconduct? *African Security Review* 26 (4): 413–433. https://doi.org/10.1080/10246029.2017.1294096.

Leighton-Daly, M. 2017. Certainty and financial crime control. *Journal of Financial Crime* 24 (4): 678–690. https://doi.org/10.1108/JFC-09-2016-0058.

Latan, H., C.J. Chiappetta Jabbour, Lopes de Sousa, and A.B. Jabbour. 2019. 'Whistleblowing triangle': Framework and empirical evidence. *Journal of Business Ethics* 160 (1): 189–204. https://doi.org/10.1007/s10551-018-3862-x.

Levi, M., and R.G. Smith. 2021. *Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19*. Barton: Australian Institute of Criminology.

Mangala, D., and P. Kumari. 2017. Auditors' perceptions of the effectiveness of fraud prevention and detection methods. *Indian Journal of Corporate Governance* 10 (2): 118–142. https://doi.org/10.1177/0974686217738683.

Maulida, W.Y., and B.I. Bayunitri. 2021. The influence of whistleblowing system toward fraud prevention. *International Journal of Financial, Accounting, and Management* 2 (4): 275–294.

Masuda, B. 1993. Credit card fraud prevention: A successful retail strategy. *Crime Prevention Studies* 1: 121–134.

Moore, T., and R. Clayton. 2007. Examining the impact of website take-down on phishing. In Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit (pp. 1–13).

N'Guilla Sow, A., R. Basiruddin, J. Mohammad, and S.Z. Abdul Rasid. 2018. Fraud prevention in malaysian small and medium enterprises (SMEs). *Journal of Financial Crime* 25 (2): 499–517. https://doi.org/10.1108/JFC-05-2017-0049.

ONS. 2023. Nature of crime: fraud and computer misuse. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse. Accessed 27 Jan 2023

Owens, E., and C.M. Jessup. 2014. Federal improper payments: An overview. *Journal of Government Financial Management* 63 (2): 489.

Peltier-Rivest, D. 2009. An analysis of the victims of occupational fraud: A Canadian perspective. *Journal of Financial Crime* 16 (1): 60–66. https://doi.org/10.1108/13590790910924966.

Prenzler, T. 2020. What works in fraud prevention: A review of real-world intervention projects. *Journal of Criminological Research, Policy and Practice* 6 (1): 83–96. https://doi.org/10.1108/JCRPP-04-2019-0026.

Rae, K., and N. Subramaniam. 2008. Quality of internal control procedures: Antecedents and moderating effect on organisational justice and employee fraud. *Managerial Auditing Journal* 23 (2): 104–124. https://doi.org/10.1108/02686900810839820.

Sapienza, A., S.K. Ernala, A. Bessi, K. Lerman, and E. Ferrara. 2018. DISCOVER: Mining online chatter for emerging cyber threats. Paper presented at the The Web Conference 2018 - Companion of the World Wide Web Conference. *WWW* 2018: 983–990. https://doi.org/10.1145/3184558.3191528.

Schwartz, R.D., and S. Orleans. 1967. On legal sanctions. *The University of Chicago Law Review* 34 (2): 274–300.

Shepherd, D., and M. Button. 2019. Organizational inhibitions to addressing occupational fraud: A theory of differential rationalization. *Deviant Behavior* 40 (8): 971–991.

Sherman, L.W., D.L. MacKenzie, D.P. Farrington, and B.C. Welsh, eds. 2002. *Evidence-based crime prevention*. London: Routledge.

Sherman, L.W. 2013. The rise of evidence-based policing: Targeting, testing, and tracking. *Crime and Justice* 42 (1): 377–451.

Sherman, L.W., D.C. Gottfredson, D.L. MacKenzie, J. Eck, P. Reuter, S.D. Bushway. 1997. Preventing crime: What works, what doesn't, what's promising. A Report to the United States Congress.

Sherman, L.W., D.C. Gottfredson, D.L. MacKenzie, J. Eck, P. Reuter, and S.D. Bushway. 1998. Preventing crime: What works, what doesn't, what's promising. US Department of Justice, Office of Justice Programs, National Institute of Justice. Retrieved from https://www.ojp.gov/pdffiles/171676.pdf. Accessed 27 Jan 2023.

Smith, M.J., and R.V. Clarke. 2012. *Situational crime prevention: Classifying techniques using "good enough" theory*. New York: The Oxford Handbook of Crime Prevention.

Soltani, B. 2014. The anatomy of corporate fraud: a comparative analysis of high profile American and European corporate scandals. *Journal of Business Ethics* 120 (2): 251–274. https://doi.org/10.1007/s10551-013-1660-z.

Spink, J., W. Chen, G. Zhang, and C. Speier-Pero. 2019. Introducing the food fraud prevention cycle (FFPC): A dynamic information management and strategic roadmap. *Food Control* 105: 233–241. https://doi.org/10.1016/j.foodcont.2019.06.002.

Tunley, M. 2011. Uncovering the iceberg: Mandating the measurement of fraud in the United Kingdom. *International Journal of Law, Crime and Justice* 39 (3): 190–203. https://doi.org/10.1016/j.ijlcj.2011.05.007.

Tunley, M., M. Button, D. Shepherd, and D. Blackbourn. 2018. Preventing occupational corruption: Utilising situational crime prevention techniques and theory to enhance organisational resilience. *Security Journal* 31 (1): 21–52. https://doi.org/10.1057/s41284-016-0087-5.

US National Institute of Justice Crime Solutions. n.d. https://crimesolutions.ojp.gov/topics/topics-and-subtopics. Accessed 27 Jan 2023

Webb, B. 1996. Preventing plastic credit card fraud in the UK. *Security Journal* 7 (1): 23–25.

White, Susan O., and Samuel Krislov. 1977. *Understanding crime: An evaluation of the national institute of law enforcement and criminal justice*. Washington, DC: National Academy of Sciences.

Williams, T. 2018. Role of management, corporate governance, and sarbanes-oxley in fraud: A focus on the precious metals industry. In *Sustainability and social responsibility: Regulation and reporting: accounting, finance, sustainability, governance & fraud: Theory and application*, ed. G. Gal, O. Akisik, and W. Wooldridge. Singapore: Springer.

Zeng, H., L. Yang, and J. Shi. 2020. Does the supervisory ability of internal audit executives affect the occurrence of corporate fraud? evidence from small and medium-sized listed enterprises in china. *International Journal of Accounting and Information Management* 29 (1): 1–26. https://doi.org/10.1108/IJAIM-02-2020-0020.

Zimring, Franklin E. 1976. Field experiments in general deterrence: Preferring the tortoise to the hare. *Evaluation* 3: 132–135.