DIPARTIMENTO
DI SCIENZE AZIENDALI
MANAGEMENT
& INNOVATION SYSTEMS

UNIVERSITA' DEGLI STUDI DI SALERNO

Dipartimento di Scienze Aziendali
Management & Innovation Systems

Dottorato di Ricerca in
Big Data Management & Innovation Systems
XXXV Ciclo

Tesi di dottorato

The Importance and Evolution of Forensic Accounting

Coordinatore
Ch.mo Prof. Valerio Antonelli

Tutor
Ch.mo Prof. Valerio Antonelli

Candidato

dott. ssa Maria Francesca Lupo

Anno Accademico 2019 - 2022

Acknowledgements

I would like to warm-heartedly thank my tutor, Professor Valerio Antonelli, for having supported me throughout this three-year journey and during the difficult times of the pandemic. Every conversation has augmented my knowledge and changed my way of thinking. I would also like to thank Professor Raffaele D'Alessio as this work would never have been possible without his guidance and his always correct advice on both research and life. Another warm thanks goes out to Professor Emanuela Cafaro which guided me and also became a good friend of mine. Nevertheless, the biggest thanks goes to my parents for having always supported me throughout all my studies and for having always believed in me strongly, even when I did not.

Dedicated to my family
and the loved ones who I wished were still here close to me

General Index

Preface

Committing any fraud, whether it is a significant scheme such as in an organization, or a small project (such as cheating), could be said that it is a phenomenon inherent in human society and accompanying it throughout the history of its existence. Many individuals do not hesitate to use all sorts of (and often bizarre) methods for circumventing rules or laws, thus promoting one's interests. Since regulations and laws are subject to constant changes, fraud methods are also changing, thus stimulating the creativity of their creators.

The field of accounting does not avoid negative manifestations of human creativity. Accounting fraud arises in companies at different levels and from different motivations. The common denominator, however, is that these motivations are always selfishness and personal gain. The initiator, for example, a company director trying to improve current results, can be a fraud in the eyes of investors or a manager manipulating the necessary parameters to achieve a higher bonus. Fraud results in financial damage and loss of credibility against a specific individual or organization. Accounting fraud is a natural and unexceptional phenomenon in today's economies.

Therefore, the issue of accounting fraud is still very current and exciting. From a more optimistic perspective, it should be emphasized that the development of fraud is also occurring in the development of methods helping to detect these frauds through forensic accounting investigators. Moreover, it is an activity that, unlike an audit, does not have a regulatory framework. However, it has a wide and exciting range of methods that explicitly focus on fraud detection.

Forensic accounting and its methods are a popular topic, especially in the foreign professional literature (especially in Anglo-Saxon countries). Domestic literature offers only a limited number of publications devoted to the methodology detection of accounting fraud.

This thesis delves deeply into fraud as well as the forensic accounting profession. It describes forensic accountants' education, training, and careers and why the demand for this profession has suddenly increased. The necessary skills of forensic accountants are discussed, such as why these skills are valuable and discussing standard forensic accounting techniques and how they can be employed to detect and prevent fraud. This dissertation tries to explain several fraud schemes and well-known frauds that contributed to the increased demand for forensic accountants. The fraud triangle, as well as other contributing factors, are investigated.

This work discusses the changes made in the aftermath of the Enron and WorldCom scandals and the Sarbanes-Oxley Act of 2002. There are interpretations for the amendments made and why they were necessary. This dissertation aims to demonstrate the significance of forensic accounting while also thoroughly explaining the various aspects of fraud and forensic accounting. Furthermore, there are highlights on the importance of strong corporate governance, explaining the COSO internal control framework, and listing and explaining several critical internal controls. Cybersecurity is also discussed, including why it has become a must-have and how companies can more effectively enforce cybersecurity measures.

The study is divided into the first chapter dedicated to forensic accounting with a great explanation of the concept and its origins throughout history, starting from the Code of Hammurabi. The second chapter regards forensic accountants explaining the

necessary education, skills and training necessary to become one and the differences between forensic accountants and auditors. Moreover, there is also a depiction of the forensic accounting process. The third chapter is about fraud, starting with the definition and answering the question, "why does fraud occur?". The various fraud schemes are portrayed, and there is an emphasis on the most famous ones with real examples. The fraud investigation cycle is also discussed at the end of this chapter. The fourth chapter is about the various types of existing forensic accounting techniques, mainly focusing on Computer Assisted Auditing Techniques (CAATs), data mining techniques, ratio analysis, Benford's law and the Theory of relative size factors (RSF). Chapter five focuses on the internal controls framework with a focus on the COSO Model of Internal Controls and the Sarbanes-Oaxley Act. Following chapter six regards the current advances made in the field of cybersecurity. Chapter seven depicts the situation of forensic accounting in Italy with all the steps taken towards this field and a discussion on the areas that need to be advanced. Lastly, there are the conclusions.

Chapter One

I. Forensic Accounting

i. What is it?

Forensic accounting definitions frequently refer to the forensic accountant's role in fraud detection, prevention, and investigation. While these definitions are not necessarily incorrect, they only describe forensic accounting in the context of fraud. Many books have even been written about forensic accounting that focuses on preventing and investigating fraud schemes and includes a wealth of fraud-related information (Silverstone et al., 2012, p. 3). To better understand forensic accounting, define the two words that comprise the definition. Webster's dictionary defines "forensic" as "something belonging to or suitable for courts of justice or public discussions and debate," but in this field of study, forensic refers to the application of financial facts to legal problems (Singleton & Singleton, 2010, p.12).

The American Institute of Certified Public Accountants 1941 defines accounting as "the science of recording, classifying, and summarizing economic transactions and events in a logical manner in order to provide useful and understandable financial information to third parties to aid in decision-making" (Accounting Verse, 2022). Following these definitions, Hopwood et al. (2012, p. 3-5) define forensic accounting as "the application of investigative and analytical skills for the purpose of resolving financial issues in a manner that meets the standards required by courts of law," while forensic accounting is defined as fraud investigation that also deals with anti-fraud controls and non-financial data collection (Singleton & Singleton, 2010, p.12). Forensic accounting skills include accounting, finance, auditing procedures, research,

quantitative methods, and investigations to be more descriptive. This activity also necessitates knowledge of specific areas of the law. Combined with these skills, forensic accountants can collect, analyze, and evaluate evidence and interpret and communicate findings (Crain et al., 2016, p. 4).

ii. The origins of Forensic Accounting

Regarding the origins of forensic accounting, it is critical to emphasize how, for thousands of years, fraud in all its forms has been a part of the business sector. The Hammurabi Babylonian Code of Laws, known as the first document dealing with laws and containing rules of commerce, religion, and daily life, is one example of the existence of fraud dating back to approximately 1800 B.C. The legislator's laws described possible scenarios involving herders and cattle, as well as how, in the event of fraud, a payment of ten times the loss was to be made to the owner (Skalak et al., 2011, p. 4).

Nonetheless, the topic of forensic accounting did not receive the expected boom or reception when it arrived in the 1970s and 1980s in the United States because prosecutors needed tools to support the provision of evidence, also due to the various loan and savings scandals of the time.

This figure was unknown until the arrival of forensic auditors in the 1990s coincided with the rise of financial scandals and fraud in the United States. There are many historians of accounting, but not forensic accounting, because, at one point in time, courts did not focus on the search for evidence to prove people's guilt, so there is a massive gap in this subject. Only in the 1930s, when an accountant helped to arrest Al Capone, there was some light shined on this matter. The protagonist in the film and

book referring to the capture of the mobster is Elliot Ness and our accountant, who could be the drama's hero, although lost in anonymity. The rise in forensic accounting began with the historic capture of Al Capone because organized crime flourished in the United States like never before during the prohibition era of liquor and gambling. Millions of dollars were made through illegal means (Louwers, 2015). The money was laundered, allowing the Master gangster bosses to live like tycoons while staying out of the hands of the law. Little justice could be done in the face of these criminal activities, and no evidence could be used against people like Al Capone, Lucky Luciano, and Bugsy Siegel.

Distinguishing illegal profits from legal sources was extremely difficult as the two would often mingle in cases of organized crime organizations. One day, an accountant in the Tax Department came up with the idea of framing Al Capone with Tax Law and then dedicated himself to searching for evidence. Suddenly, an abundance of evidence was discovered while reviewing the accounts of a business that washed and even ironed Al Capone's money. He was the first subject being convicted using the Internal Revenue Code which utilized the net worth method to uncover unreported income that was to be taxed (Manning, 2005, p.596). The Prosecutor's Office obtained the money launderer and the payment book, allowing them to verify that the volume of sales exceeded the theoretical capacity of the washers' business; in fact, the actual sales volume and the declared sales volume differed significantly. Although Al Capone's murder, extortion, and other crimes could not be proven, however, forensic accountants and auditors could demonstrate tax fraud, allowing the organization to be dismantled (Crain et al., 2016, p.6).

The FIRREA introduced in 1989 (Financial Institutions Reform, Recovery, and Enforcement Act) (FRASER, 1989) managed to boost the authority of the Federal Finance Board and, following the failure of relevant public organizations, led to the increase and aid of the rise of Certified Public Accountants (CPA) who became the official specialists in antifraud whose scope was to implement internal controls. As a result, forensic audit arises from errors, fraud, and embezzlement in companies where designated resources are not used for the advancement of the community, resulting in a higher level of poverty and unemployment (Rechtman, 2020). This situation occurs because the assigned positions are filled by evil people who do not comply with the standards proposed by law, resulting in a misuse of the resources granted for developing projects focused on welfare.

Chapter two

II. Forensic Accountants

i. Education and training

Forensic accounting investigators merge their accounting knowledge with investigative skills in various investigative accounting and litigation support settings. They work for public accounting firms' forensic accounting divisions, risk consulting and forensic accounting consulting firms, legal professionals, agencies of law enforcement insurance companies, government organizations, or financial institutions.

Therefore, one must have a bachelor's or master's degree in forensic accounting, accounting, finance, or a related field to start the forensic accounting career path. A background study or experience in law enforcement or criminal justice is considered advantageous. Many companies encourage employees to obtain the CFE credential and the Certified Public Accountant (CPA) or Chartered Accountant license (CA). Additionally, to the university degrees, the licenses consist of training, as open forensic accounting positions usually require a certain level of experience (around three years of experience in the accounting field). Training is crucial due to the various responsibilities the forensic accountant has that no other fraud auditor has to worry about. The conduction of forensic analysis, the performing of forensic research, and the preparation of forensic reports with the necessary analytical data are also tasks that the forensic accountant can exclusively conduct (ACFE, 2022).

ii. Important skills

It is crucial to underline the importance of the role of forensic accounting and all the skills and expertise which is required even to consider practicing this job, or else the above-mentioned circumstances would not even exist. Forensic accounting covers various branches and educational areas, some of which overlap. As Crain et al. (2016) state in their book, there are several areas a forensic accounting has to cover; the most important ones are accounting and auditing, but the following one can also focus on the importance of criminology, investigation, communication, accounting information systems, and information technology, as well as risk analysis, psychology, problem-solving and knowledge of the legal system.

Society expects more significant results from investigators that reduce impunity, especially in these difficult times when organized crime uses more sophisticated means to launder money, illicit finance operations, and conceal the outcomes of its various crimes. The financial audit is the most traditional, well-known, and widely used of all audits, and it is legally required for many businesses, giving rise to the auditor profession. If fraud is discovered, the auditor must determine the impact on the results of the financial statement. A financial auditor does not investigate fraud beyond the evidence to determine its prevalence in the audited balances. The forensic auditor oversees investigating financial fraud detection and prevention.

Different skills are necessary or just helpful for the forensic accountant's role, skills that are not required for fraud auditors. Crain et al., in their book "Essentials of Forensic Accounting" (2016), have created a list of skills that are required for the role of forensic accounting investigator as follows: accounting, auditing, investigative skills, digital forensics and criminology, accounting information systems, risk analysis,

communication skills, psychology background, information technology, problem-solving skills, and legal background knowledge. Starting from the first skill, accounting knowledge is required as although a forensic accountant specializing in occupational fraud may not need to be an expert in international accounting standards, he or she will almost certainly require specialized knowledge and skills in accounting information systems, digital forensics as well as business valuation skills. Auditing is essential to this role as when forensic accountants give testimony as expert witnesses before a trier of fact, they usually express their research results as expert opinions. Their conclusions must be supported by evidence, which must be gathered and interpreted.

The various types of evidence that may be gathered, how and where to preserve the legal rights of those under investigation, their chain of custody as well as how to identify various types of fraud schemes, how to conduct interviews, and how to detect deception are all part of the investigative skills required by forensic accountants. Furthermore, the authors include digital forensics and criminology as the forensic accountant should have a basic understanding of the various functions provided by forensic investigators, digital forensics experts, criminologists, forensic laboratories, prosecutors, and attorneys in criminal investigations. It could be stated that nowadays, almost all crimes involve digital devices, including computer systems. As a result, it is advantageous for the forensic accountant investigating fraud to have a basic knowledge of digital forensics in computer and network forensics. This string of thought also brings to the accounting information systems knowledge as internal fraud schemes usually involve the infraction of weak or inconsequential internal controls within specific business processes, requiring the forensic accountant to understand internal control processes and how they interact with organizational processes and the accounting information system.

Regarding risk analysis, forensic accountants are frequently involved in fraud risk management because they are responsible for the steps of fraud detection and prevention, as well as response to fraud. Furthermore, communication skills are extremely crucial since they are in direct contact with the active subjects of the fraud. They must have communication skills that are not required in the professional profiles of the external auditor and the fraud auditor. Only by having a strong ability to adapt to different attitudes and a broad mindset will the forensic accountant be able to converse with the interviewees and gather as much information as possible from them. This very simplistic view of the forensic accountant's interviews ignores the psychological and technical background required for the overall investigation's success, which brings attention to the importance of psychology knowledge. In financial fraud cases, obtaining a confession begins with gathering documentary evidence, then moves on to interviews with non-suspects, and often concludes with an interview with the prime suspect. The ability to distinguish between honesty and deception is essential for interview success. As a result, forensic accountants are sometimes assisted by using psychological techniques, such as analyzing body language and eye movements (Ibid, p.8).

Information technology knowledge is inextricably linked to the significance of digital forensics and accounting information systems since technology is constantly changing and is an unavoidable component of several forms of forensic accounting practice. They not only use cutting-edge technology in their investigations, but they must also be cognizant of evolving technological advancements to maintain current professional skills. Following the more technical skills, the authors highlight the importance of problem-solving skills; forensic accounting investigators are constantly confronted with mysteries and riddles that provide opportunities to hone their critical-thinking abilities as there always is an opposing side in fraud investigations, litigation,

and dispute resolution. In many cases, the opposing side is incredibly smart and strives to mislead and conceal the truth. Lastly, the term forensic itself has to do with the law. Therefore, it is crucial to underline how forensic accountants perform litigation services and have the main role in legal resolution processes.

Furthermore, several studies have underlined how important and beneficial the study of forensic accounting and its skill is. For instance, Alshurafat, in his work (2021), shines a light on all the valuable knowledge, skills, and abilities that forensic accounting scholars are exposed to. He explains how various experimental studies have depicted a clear image of the rise of employment opportunities for forensic accounting studies after graduation, as well as how their anti-fraud knowledge is considered more beneficial in the work environment than that of a simple auditing course. Furthermore, other studies have shown how forensic accounting students tend to have a high level of skepticism and creativity compared to other students. The study of forensic accounting is crucial and beneficial to all accounting disciplines, regardless of the prospective career path one may decide to embark on.

Furthermore, emphasis could be brought on forensic accountants' moral and intellectual virtues, as various studies have observed in the past. As described by Howieson (2018), there has been interesting prior literature, including surveys on the topic of personal attributes and work skills of forensic accountants. Regarding personal attributes, the leading five adjectives used for a good forensic accountant were inquisitive, analytical, intelligent, interpersonal, and engaging, which somehow correspond to Aristotle's characterization of the virtues as moral and intellectual (Ibid, 2018, p. 158).

Lastly, prior researchers have confirmed that the advantages of forensic accounting stem from the wide range of responsibilities that fall under the forensic accounting

umbrella and are regarded as an essential profession because it requires a diverse set of skills that are crucial in combating today's new everchanging fraudulent behaviors (Tiwari, 2017).

iii. Differences between forensic accounting and auditing

Auditing and forensic accounting may seem like intertwining branches. However, there are various factors differentiating them from one another. The forensic accountant enters a fraud case later than the fraud auditor, when there is already suspicion or evidence of an illegal act. In practice, the first play a reactive role, whereas the second is actively involved in preventing and detecting fraud. Accordingly, the forensic accountant and the auditor should not be confused. Although the forensic accountant needs to have a robust auditing background and knowledge, it is not enough to practice this role. It could be stated that the auditor's focus is to examine an entity's financial statements and ensure that such statements are presented truthfully in all material respects (Golden et al., 2006, pp. 40-42). The auditor's responsibility regards implementing and designing sufficient audit procedures for correctly detecting possible deficiencies in a company's financial statements. The auditor's role is then to efficiently detect possible errors in financial statements (material misstatements), and correct such misrepresentations before such statements are publicized.

Crain et al. 2015 also distinguish between forensic accounting and traditional Accounting. Traditional accounting, according to them, entails recording, categorizing, analyzing, and reporting financial data and information. When using a financial reporting framework, the emphasis is on converting raw financial data into useful information for decision-makers. Financial statements are commonly used to present helpful information to borrowers for decision-making. In short, the traditional

accountant's work product is one or more financial statements. On the other hand, the typical work of forensic accountants differs significantly from that of traditional accountants.

As stated by Kaur in his work "A systematic review on forensic accounting and its contribution towards fraud detection and prevention" (2022); various reports that auditing firms have published in the past years have admitted that in order to both detect and prevent fraud, forensic accounting techniques must be incorporated, especially in emerging economies, as proven by the author. Even though various governments worldwide have issued strict guidelines on the ethical code for companies to follow, great fraud scandals still occur. Furthermore, the author also points out that external auditors are technically not responsible for detecting financial statement fraud, leading to an ever-growing demand for the role of forensic accountant.

The forensic accounting investigator has a distinct set of concerns based on different roles that necessitate various tools, thought processes, and attitudes. The fear of the forensic accounting investigator is not to reach a general opinion on financial statements derived from reasonable efforts within a reasonable materiality boundary. Instead, the forensic accounting investigator is concerned, at a much more acceptable level, with the detailed development of factual information about the who, what, when, where, how, and why of a suspected or known impropriety derived from both documentary and testimonial evidence. In most cases, sampling and materiality concepts are not used to determine the scope of forensic accounting procedures. Instead, all pertinent evidence is sought and scrutinized (Golden et al., 2006, p. 41).

Based on the investigation's findings, the forensic accounting investigator implements corrective actions, which frequently include changes in accounting processes, policies, and personnel actions when assessing and measuring losses or any

other possible damage to a company. Furthermore, the forensic accounting investigator takes preventive measures to ensure that the problem does not reoccur (Golden et al., 2006, p. 42). The findings and recommendations of the forensic accounting investigator may be used as evidence in litigation or criminal proceedings against the perpetrators. While the forensic accounting investigator's findings are often damning, corrective actions may also result in positive organizational changes. For example, by implementing new accounting practices, the investigative findings may result in lower taxes and increased profits. Preventive measures like regular audits can help ensure that criminal activity does not reoccur. The forensic inspector should evaluate fraud from the standpoints of the environment, culture, law, audit, and perpetrator. While these individuals must be able to apply "Generally Accepted Accounting Principles" to commercial transactions, they must also possess the independence, objectivity, and professional scepticism expected of auditors as expressed in "Generally Accepted Auditing Standards" His responsibilities also include preparing a report for the competent judges that explains what happened: in essence, the forensic accountant is in charge of preparing a possible legal case and thus of gathering evidence and testimonies to support the discovered fraud. He must therefore combine his accounting skills with investigative and communication skills; the latter, in particular, clearly distinguish this professional from the financial auditor and the fraud auditor, as only the forensic accountant is necessary to translate complicated financial transactions and numerical information into terms understandable by people who do not belong to the financial world, such as judges, lawyers, or jury members. (Singleton & Singleton, 2010, pp.13-14). Therefore, it could be stated that the forensic accountant is expected to be more knowledgeable than the auditor.

iv. The forensic accounting process

Forensic accounting is generally categorized into two main areas: litigation services and investigative services. Concerning the first topic, forensic accounting employs its experts to testify as an expert or non-testifying consultants, as well as to provide aid for actual or prospective legal or regulatory deliberations prior to a trier of fact in connection with the resolution of disagreements between sides. The solutions included in the litigation services include; Serving as expert testimony, litigation advisor, and various other roles in dispute settlement or legal processes. Regarding the second area, investigative services, the part of the forensic accounting experts serves as a counselor in instances that do not involve actual or threatened litigation but do implicate conducting analyses or inquests that may necessitate the same abilities as those required for litigation services (Crain et al., 2016, p.4).

Singleton et al. (2006) identified a genuine investigative process, which consists of typical steps followed by the forensic accountant in his activity. The discovery of clues, often completely by chance, is undoubtedly the first step in the investigative process. However, the fraud is not always easily identifiable, partly due to the difficulty of gathering evidence; in such cases, the forensic accountant must adopt a theoretical approach to the fraud itself, i.e., not recognizing yet which reference frame has been adopted by the offender, he must try to trace back all the known categorisations, in the hope, by exclusion, of arriving at the scheme that better serves the real case.

This stage of the investigation, which is usually carried out using the brainstorming technique, allows the forensic accountant to gain a deeper understanding of the situation and may also serve as a foundation for the development of the fraud investigation. Once the fraudulent act has been focused in general terms, the forensic accountant will try to

verify the existence of the fraud by accumulating interviews with more or less subjects involved in the case, which may then represent legal evidence, using the documentary evidence collected by the fraud auditor during the course of his activity.

The ACFE and various specialist texts refer to this professional figure as a "fraud examiner," but his scope of action can extend far beyond fraud. The AICPA's Code of Professional Conduct combines these "investigative services" with those provided in support of one or both parties in a legal dispute - or as an arbitrator. The AICPA defines forensic accounting as non-attesting services that necessitate the application of unique technical skills in the fields of accounting, auditing, finance, quantitative methods, and specific areas of law, as well as research and investigative skills designed to collect, analyze, and evaluate evidence and to interpret and communicate what is discovered, which includes litigation services and investigative services (AICPA, 2014).

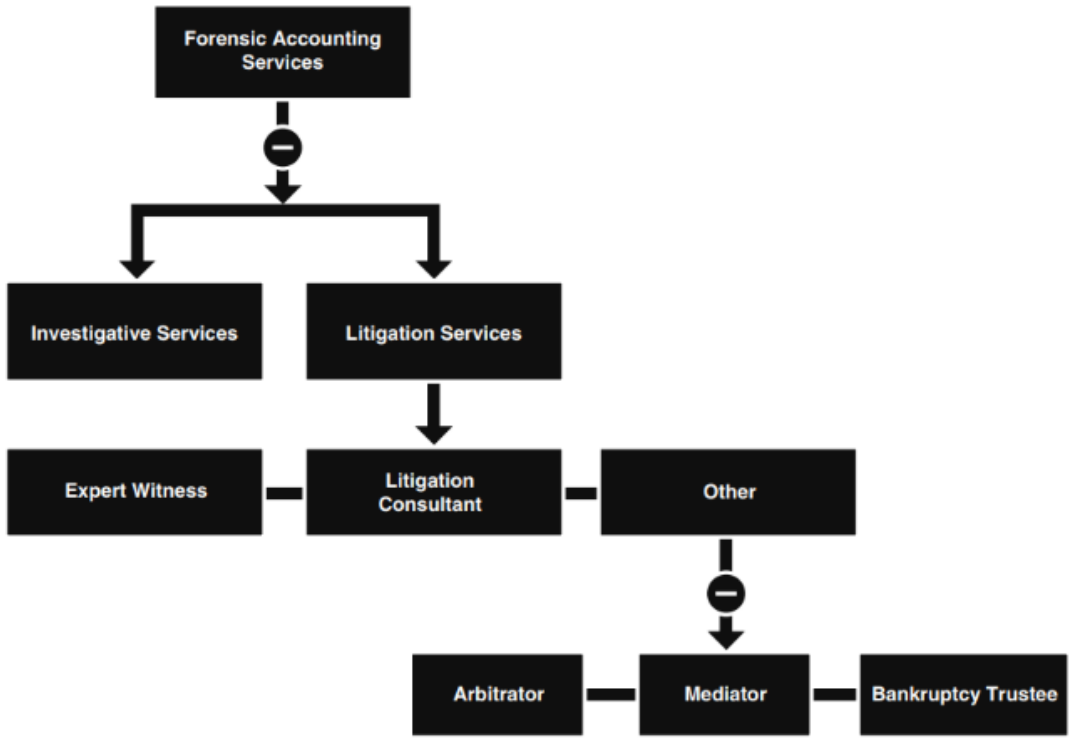


Fig. 1 – "Forensic Accounting services"[1]

[1] Forensic accounting scheme retrieved from page 190 of Crain, Michael A., William S. Hopwood, Richard S. Gendler, George R. Young, and Carl Pacini. (2015). "*Essentials of Forensic Accounting*." New York, New York: American Institute of Certified Public Accountants inc.

While the investigative services are primarily concerned with the actual investigation of fraud (and possibly a minor part of the detection of the same), the litigation services recognize the role of the consultant as an expert who gathers evidence in support of the resolution of a dispute between several parties over an actual or potential cause.

There are three types of litigation services: expert witness, a professional opinion is required but not on a fact or event, litigation consultant, and other services (such as arbitration or mediation). This combines fraud investigation services with other possible professional services for the same professional, such as penalty analysis, professional standards analysis, economic damage calculations, business valuation, pension valuation, intangible valuation, and bankruptcy advice. Furthermore, it offers services such as the analysis of marriage disputes, historical results, accounting in particular areas, clause and contractual costs, anti-trust, insurance claims, and dispute attestation.

Regarding the investigative side of forensic accounting, the main points of its definition include the fact that it is a branch of accounting commonly referred to as (accounting) but which requires specific and distinct techniques that a generic accounting profession does not require, that it has strong links with the law because it is a discipline linked to a civil or criminal case and, thus, to a court, and finally that it is a discipline of interpretation and analysis. What is implied is that the most essential skill required of a forensic accountant in the investigative field will be that of possessing a mentality aimed at research (even less scientific but more intuitive) of the mechanisms by which fraud is carried out: discovering them can sometimes be considered an art and not science because it requires both rigorous works - and in this sense, the determination, persistence, and patience mentioned above return. Other technical skills emphasize the forensic accountant's ability to identify fraud with minimal initial information, interview, know and understand the evidence, write reports, and use the

previously mentioned investigative techniques.

As many authors have already explained in their works, the point of parity in a regular audit is that everyone is telling the truth, that the documents are not forged, and that the books and scriptures have not been deliberately manipulated. In contrast, in a forensic investigation, the starting point is entirely different. The forensic accountant's only question is: how far and wide will they have gone to manipulate the records? (Young, 2006). Forensic accountants will use their investigative skills to identify those responsible for the discovered illegal behavior and its duration, nature, scope, and financial impact. A significant portion of all of this is the formal review of email content and documentation, with the added benefit of having an external and objective look at what happened, who was responsible, and why it occurred (an external expert will always be more credible than an internal accountant in carrying out investigations). The forensic accountant's initial steps are always standard, and an initial meeting is held in order to discuss, with the investigation team, the nature of the possible fraud, the places to visit, what resources are needed, and the type to be analyzed, as well as the accounting system (all those requests made to management during the assignment of the assignment). Second, a work plan and a budget are developed and communicated, with explanations and justifications for each modification. Finally, a list is created to understand how the team will divide the investigation tasks. Each member must be introduced to a trusted person within the organization as the point of contact for his or her requests. The team will then meet regularly to discuss the obstacles discovered and the following steps (AICPA, 2009, p.120).

The area of expert witness testimony entails evaluating some issues that the court must examine, reaching an appropriate conclusion within the framework of the relevant legal legislation, and submitting the result to the judicial authorities both in writing and

verbally, meaning that an expert witness is a person with specialized knowledge whose work is accepted by judicial authorities to assist in resolving a dispute or revealing the truth (Brennan, 2005).

According to the AICPA, an expert witness is a person with specialized knowledge, experience, and training who can provide scientific, technical, or specialized information on a subject or contribute to clarifying an event. In this regard, the forensic accountant is the individual who notifies the judicial authorities about the technical problems related to the case that fall under his specialty (AICPA, 2009).

Chapter three

III. Fraud

i. What is fraud?

Before delving more into the current topic of corporate fraud, it is probably nearly necessary to establish a definition of fraud, which will undoubtedly fall short of many people's expectations. The problem is that, given the issue's complexity and, more importantly, its ever-changing character, it is impossible to encompass all sorts of fraud in a single description. To better understand the issue and the many and varied manifestations of fraudulent activity in general, as well as corporate fraud in particular, as a first step, it is still a good idea to explain what the term means. However, in order to progress in the study of the subject and gain a better understanding of the various and innumerable manifestations of fraudulent behavior in general and corporate fraud in particular, it is still necessary to explain the concept of fraud in order to identify its essential and qualifying features as a first step.

In common vocabulary, fraud is an act committed to injuring another person's right through deception to gain an advantage. In business practice, the phrase has a different and broader definition, encompassing all activities that obtain profits or benefits unlawfully and dishonestly, inflicting harm to others, even indirectly, and depleting value from a business. The official definition reported in the ACFE for fraud is any activity where a person lies in order to deprive an organization or a person of their money (most commonly) or property (2022). The fraud is thus carried out in a very linear manner: the plaintiff (active subject) deceives the victim (passive subject) and obtains an unfair advantage for himself or others while also causing an equally unjust

injury to the victim or others (Allegrini et al., 2003, p.60). Nevertheless, fortunately fraud can also be detected in advance as shown in the following paragraphs. For instance, suppose a financial statement analysis reveals abnormal growth in the ratio of receivables to total daily credit sales with a comparable company and the ratio of net revenues to net sales exceeds industry standards when compared to industry standards. In that case, these are early indicators of fraud. As a result, a forensic accountant's industry knowledge speeds up the research process in examining manipulated financial statements and gathering data (Gaither, 2018, p.14).

In terms of internal auditors, while performing their assurance or consulting duties, they may come across evidence of financial fraud, so they must have sufficient knowledge to identify fraud indicators. However, they should not expect the same knowledge as someone trained to detect and investigate fraud. The greater the risk of fraud in an organization, the more critical it is that some internal auditors are forensic auditors. In its beginnings, forensic auditing was applied in the investigation of fraud in the public sector, considering real support to the traditional government audit, especially in the face of crimes such as illicit enrichment, misappropriation of funds, bribery, corruption, embezzlement, prevarication, conflict of interest, etc. However, forensic auditing has not been limited to administrative corruption fraud but has diversified its portfolio of services to participate in investigations related to financial crimes, corporate crime, money laundering, and terrorism, among others. In this sense, the forensic auditor can work both in the public and private sectors, providing procedural support ranging from collecting evidence to expert opinion. Similarly, their work stands out not only in ongoing investigations but also in stages before fraud; that is, the public accountant acts toward conducting investigations and calculations that allow

determining the existence of a crime and its amount to define the beginning of a judicial process is justified (Navarrete & Callego, 2022 and Silverstone et al., 2012).

ii. Why does fraud occur?

Any individual can commit fraud, and the PwC study proposed a composite portrait of the fraudulent employee, who is, in most cases, a man with an executive function, between 31 and 40 years old, with seniority of three to five years within the company (2016). In most cases, it is a collaborator who is well-liked by his colleagues and has the trust of the hierarchy who commits business fraud. Surprisingly, it demonstrates that the fraudster is frequently someone that can be described as expected at first but is pushed to commit the act due to various psychological factors that will be discussed later.

Another KPMG study (2016) provided a typical profile of corporate fraudsters. It turns out that their proposal is similar to PwC's in some ways. According to KPMG, a fraudster is a man between the ages of 36 and 55 in 79% of cases. It is an internal company employee in 65% of cases and a person with company responsibilities in 67% of cases. These two proposed profiles emphasize the significance of middle management because they frequently have access to a large amount of sensitive information and have a more remarkable ability to circumvent the controls that have been put in place (Management override).

Enron, Siemens, Parmalat and Volkswagen are four of the most notable examples of large organizations that have attempted and sometimes failed to overcome the devastating consequences of the emergence of fraud. It is estimated that approximately 5% of all revenues of U.S. companies are lost annually due to fraud (ACFE, 2022), but

as the case of the German car company has demonstrated, the effect on the company's reputation is the most to be feared. The four mentioned are flanked by an impressive number of companies that face the problem every year, though precise numbers are difficult to obtain due to the difficulty in bringing out a phenomenon that tends to be underestimated by its very nature. This is due to companies' challenges in identifying specific types of fraud and their standard (but not universal) reluctance to publicize the incident externally.

To summarize, the key elements required to discuss fraud are the actor and the victim (subjective factors), deception, unfair gain, and/or damage (objective elements). The scam is thus carried out in a very linear manner: the plaintiff (active subject) deceptively misleads the victim (passive subject) and obtains an unfair advantage for himself or others while causing equally unjust harm to the victim or others.

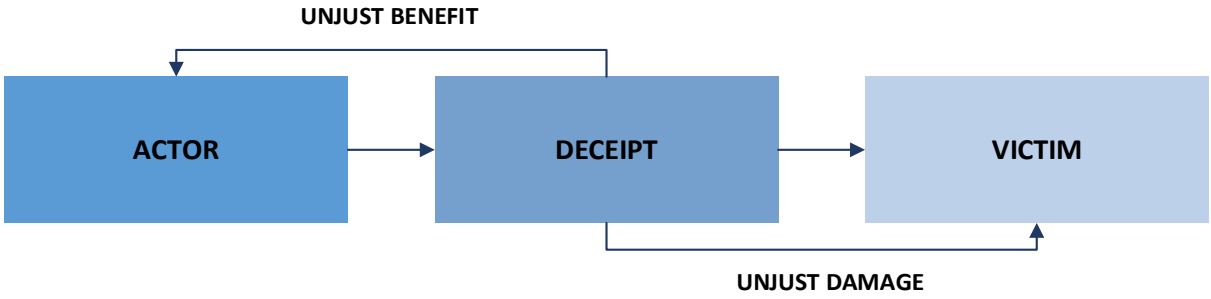


Fig. 2 – "The beginning of a fraud" [2]

In business management, the term fraud must be understood broadly to include any active or omissive behaviour that results from a recipient error and results in undue profit and damage, even potential. As a result, fraud frequently overlaps with incorrect and unfair conduct, to the point where even the agent's failure to report a pre-existing

[2] The beginning of fraud scheme adaptation taken by Allegrini M., D'Onza G., Mancini D., Garzella F. (2003). *Le frodi aziendali. Frodi amministrative, alterazioni di bilancio e computer crime (Corporate frauds. Administrative frauds, statement alterations and computer crime)*. 7° Edition. Milan:
Franco Angeli.

error committed by the victim appears to qualify an act as fraudulent. Within the broad category of corporate frauds, various crimes of varying nature and complexity can be included, such as corruption, mismanagement characterized by premeditated expedients, unauthorized risk-taking, manipulations, thefts, and others. However, corporate fraud can be divided into two broad categories: fraud committed against the company and fraud committed for the benefit of the company. The company is the victim in the first hypothesis, while it is the beneficiary of the fraudulent activity in the second. While it is not difficult to imagine cases of the first species, it may be more difficult to envision situations in which fraud is committed solely for the benefit of society. Some examples include tax evasion, violation of environmental regulations, false advertising and propaganda of the product or service offered, and the establishment of fictitious prices (Singleton et al., 2006).

The Fraud Triangle

How can fraudulent financial information be obtained? There is a specific theory that explains it from the psychological standpoint of the fraudster who applies this crime, which is sustained in opportunity, motivation, and rationalization (Cressey, 1972), also known as the “Fraud Triangle Theory”, which is drawn in the shape of a triangle, as its name implies. Fraud occurs at various levels in a wide range of situations. Each of those who commit offenses has their motivations and opportunities; however, some common elements that characterize all fraudulent behaviors can be identified. Cressey's theory to this day is the most suitable to answer the question: "why is fraud committed?" following an empirical investigation on fraud carried out in the 1950s. According to this theory, every fraud has three distinguishing features: the pressure to

commit crimes caused by the perception of a variety of needs, the rationalization mechanism, and the opportunity to commit fraud and conceal the crime while avoiding any possible sanction (Homer, 2020).

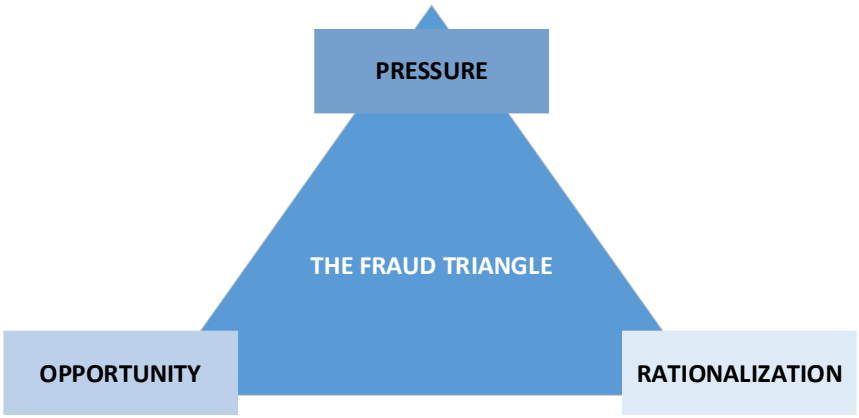


Fig. 3– Donald Cressey's fraud triangle [3]

By pressure, what is meant is an incentive. This motivation has intervened in the private life of the person willing to commit or commit fraud and has created an urgent need for resources, usually monetary. These needs are typically driven by financial distress; however, there may be instances where entirely different factors drive the pressure. Such factors include incentives dictated by a socio-political situation that can drive the active subject in the fraudulent process to act dishonestly to achieve goals related to his ego and its ideologies (Singleton et al., 2006).

The other determinant identified by Cressey is the rationalization mechanism, which is the actor's ability to initially justify the fraud committed to himself and, if discovered, to the other members of the organization. Rationalization occurs before and during the crime, endangering the subject's ethics. The most common type of rationalization involves transforming the crime (for example, cash theft) into another action (for

[3] Re-creation of the fraud triangle by Donald Cressey 1953 (image inspiration from Gamlath , M. M. S., Ab Yajid, M. S., & Khatibi, A. (2018). The New Fraud Triangle Theory - Integrating Ethical Values of Employees. Retrieved from http://ijbel.com/wp-content/uploads/2018/08/ijbel5_216.pdf)

example, a temporary loan obtained by the company), thereby finding a justification for the criminal behavior. Other common forms of rationalization encourage the individual to minimize the extent of the dishonest action ("There are people who do worse"), to see the act as compensation for the injustices suffered ("They deserve it because they exploit me"), to generalize the problem ("everyone does it"), or to construct alibis to justify the unlawful act (such as severe personal problems, usually monetary) (Singleton et al., 2006 and Golden et al., 2012).

However, trusting relationships between the various levels of the organization are necessary for the company to function. As a result, to deal with the inevitable increase in the risk of fraud caused by more extraordinary powers granted to personnel, the functionality of the control mechanisms becomes increasingly essential, as does monitoring their adequacy and effectiveness over time. It should be noted that the likelihood of committing one fraud is directly proportional to the length of the employment relationship with that particular company, for the reason that a multi-year collaboration allows individual subjects to become aware of the system's internal control weaknesses and shortcomings, providing them with a higher potential opportunity to engage in fraud. The fundamental reasoning for the fraudulent activity, the element of the human mind, and individual behaviors (the wrongdoer's capability to commit the fraud) are frequently unrecognized and unnoticed. Nevertheless, these three elements do not guarantee that fraud will occur, as stated by Pedneault & Rudewicz (2012). For instance, professor Dellaportas in 2013 decided to analyze and somehow “check” whether this fraud triangle model had any real validity after many years had gone by. This professor's study seeks to understand why accountants commit fraud by listening to their explanations of events, particularly those relating to factors that trigger their fraudulent behavior. His investigation looks into how well the Cressey triangle

represents white-collar crimes committed by accounting professionals. The information was gathered during visits to two prisons, Prison Dhurringile and Prison Loddon, in Victoria, Australia, and interviews with specific inmates. All of them were professional accountants at the time of their offenses. The interviews targeted men aged 35-60 who were previously employed in public accounting. They had the following characteristics: no history of dishonesty, greed, or gambling as motivation, stable employment, and specifically, they had to have acted alone. The inmates were found guilty of "deception"-related offenses such as embezzlement, tax evasion, check fraud, and financial statement fraud. The interviews focused on three aspects of the fraud triangle: "Why did you commit fraud under duress? How did you explain your illegal behavior? How did you expect to go undetected with the fraud?".

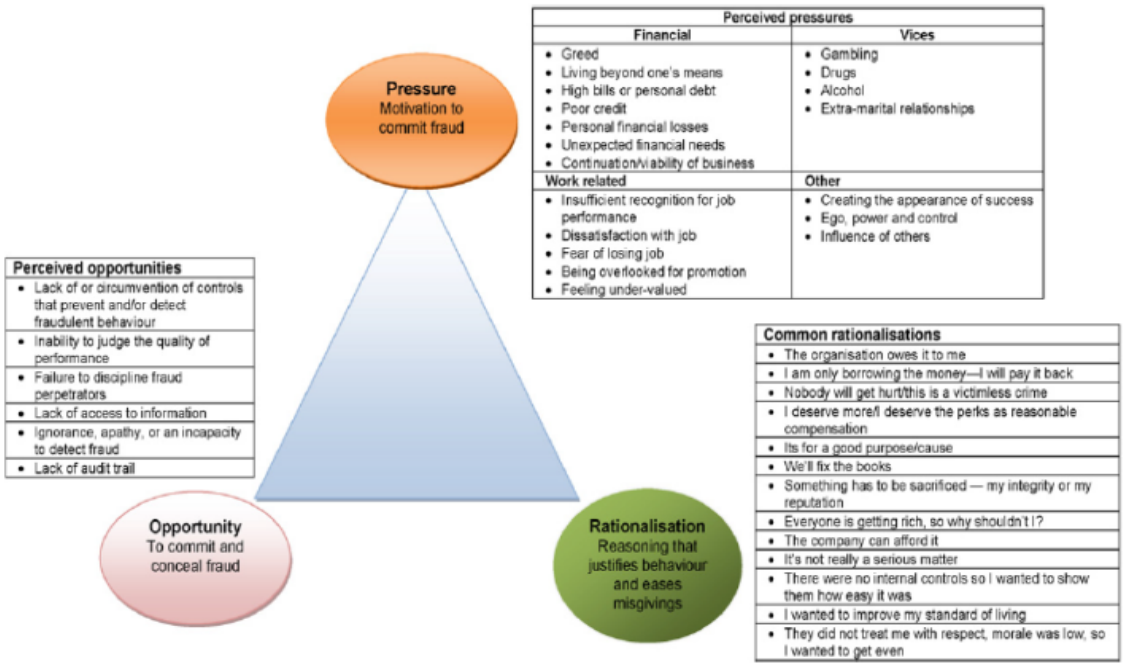


Fig.4 - Dellaporta's re-adaptation of the fraud triangle[4]

[4] Dellaporta's re-adaptation of the fraud triangle scheme retrieved by Dellaportas Steven. Conversations with inmate accountants: Motivation, opportunity, and the fraud triangle. Accounting Forum, 37(1), 2013.

The findings of this study suggest that opportunity is the primary motivator for fraudulent behavior, casting doubt on the traditional theory of equilateral triangle fraud. Even with small sample size, it has been demonstrated that an opportunity rather than motivation influences the distribution of criminal behavior, providing a better predictor of crime. Fraud occurs when the right person with the right capabilities is in the correct position: thus, fraud is typically perpetrated by senior and trusted professionals rather than junior professionals. Dellaportas favors changing the shape of the fraud triangle from an equally-sided model to an irregular model with expanded opportunities based on occupational status, as illustrated in the figure (Dellaportas, 2013).

As Duffield and Grabosky (2001) explain in their book “The Psychology of Fraud”, behavioral scientists have yet to identify a psychological trait that serves as a valid and reliable predictor of an individual's proclivity to engage in fraudulent behavior. Certain studies, however, have shown that specific characteristics and personality traits make fraud more likely. For instance, Wolfe and Hermanson (2004) have included a fourth component to Cressey's triangle, transforming it into the fraud diamond. The article "The Fraud Diamond: Considering the Four Elements of Fraud" explains how the likelihood of fraud is directly related to an individual's personality traits and capability. The traits listed that they mainly found associated with the capability element are positioning, intelligence and creativity, ego, coercion, deceit, and stress. According to the authors, the subject's position or function within the organization may provide the opportunity to create or exploit a fraud opportunity. Hence, someone in a position of authority will have more influence over specific situations or the environment.

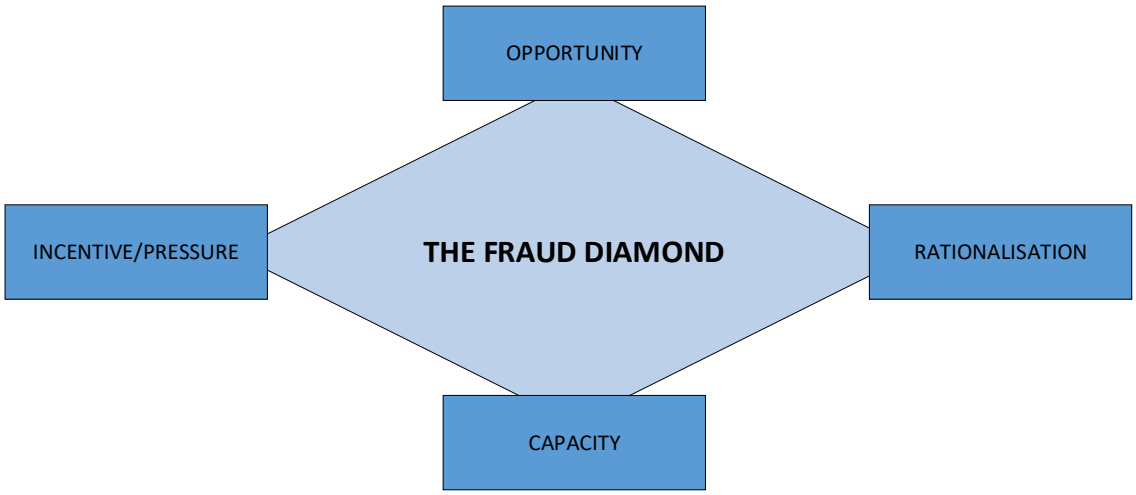


Fig. 5 – Wolfe and Hermanson's fraud diamond depiction[5]

Regarding intelligence and creativity, it is logical to assume that these qualities will be used to deceive or manipulate others to achieve the most significant advantage possible. The ego of the individual interested in fraud may be greater than that of the individual not interested in fraud as the personality traits of the former depict someone narcissistic, self-absorbed, and very confident. Regarding coercion, the subject usually has persuasive power over others. It may be able to use this power to convince or coerce others to perform with them or to pretend nothing is happening. This trait goes hand in hand with deceit, as effective and consistent lies are required for successful fraud. Lastly, the individual interested in fraud must be able to withstand stress in order to pull off the plot successfully. According to the authors, evaluating the capability element and the six common traits through investigative due diligence will aid in the prevention and detection of fraudulent activity (Wolfe & Hermanson, 2004).

[5] The new fraud diamond re-creation by Wolfe, David T., and Dana R. Hermanson. *"The Fraud Diamond: Considering the Four Elements of Fraud."* CPA Journal 74.12 (2004): 38-42.

ii. The fraud tree

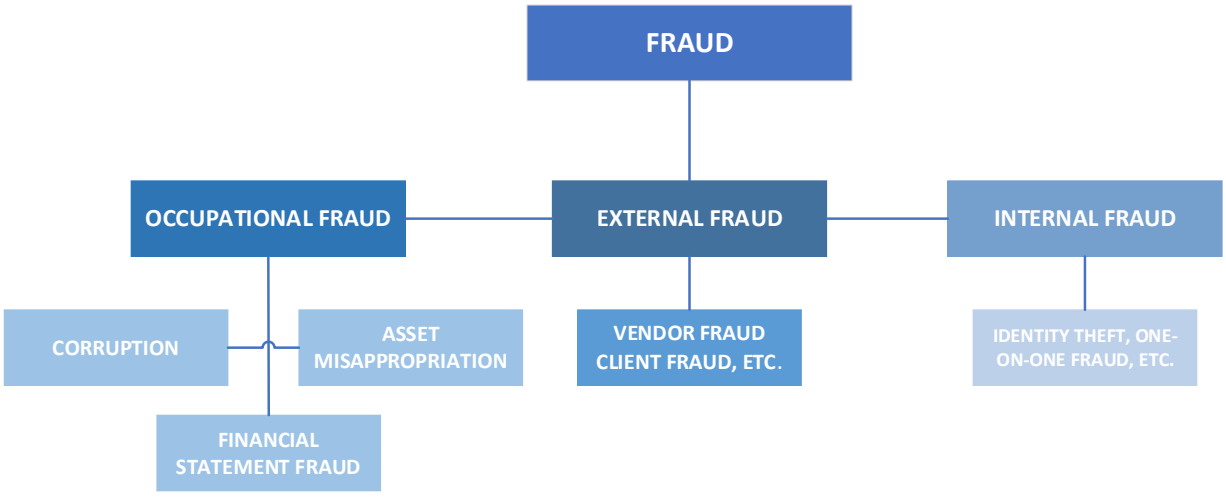


Fig. 6– The fraud tree [6]

For the purpose of forensic accounting research, it is crucial to understand what is intended with economic and financial fraud. All fraud schemes of this type can be divided into three broad categories: individual, internal, and external fraud. Individual frauds are arguably the most well-known and include systems that even readers are now familiar with email phishing, attempted security fraud against individuals, and theft of personal information, such as the "Ponzi scheme." Internal fraud, also called employment fraud, occurs when the employees are defrauding the company. Lastly, external frauds involve the company but are generally committed by bodies of individuals outside the company (such as suppliers or hackers).

External fraud can be committed by anyone with whom the organization has contact, including customers, distributors, business associates, and members of the general public. Clients opening an account with false information is one example, as well as false credit information, distributors delivering subpar supplies; business

[6] Re-creation of the fraud tree as depicted by Crain, Michael A., William S. Hopwood, Carl Pacini, and George R. Young. 2016. *Essentials of forensic accounting.* http://www.vlebooks.com/vleweb/product/openreader?id=none&isbn=9781119552260 in page 246.

associates leaking trade secrets; and the public hacking into the company's computer network (Crain et al., 2016).

However, when discussing economic and financial fraud, usually the focus is on the most relevant and exciting category: internal or occupational fraud, in which the scammer is a company employee. Such fraud schemes are divided into mainly three macro-categories: asset misappropriation, corruption, and financial statement fraud.

iii. Fraud schemes

The Association of Certified Fraud Examiners also outlined the so-called "fraud tree," which contains 49 typical schemes and has remained stable over time, serving as a point of reference for anyone working in the field despite scammers inventing new and increasingly sophisticated techniques, mainly thanks to the technological factor (ACFE, 2022).

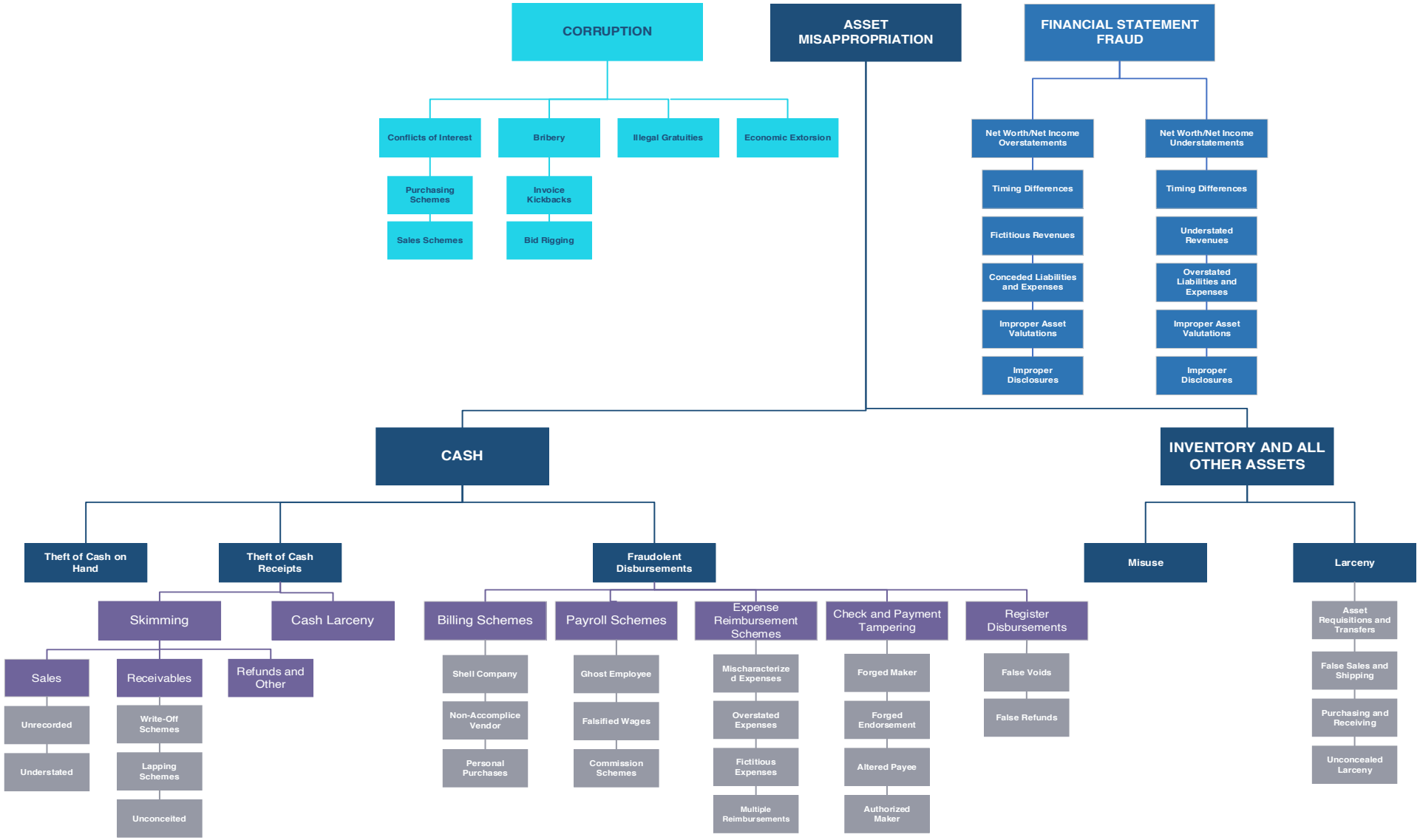


Fig. 6 – Recreation of ACFE Fraud Tree [7]

[7] Re-creation of the ACFE Fraud Tree as depicted on page 10 of Association of Certified Fraud Examiners. (2022). "*Report To The Nations On Occupational Fraud And Abuse".* Global fraud study. ACFE.

In addition to the numbers provided, approximately 20 of the 49 proposed schemes cover 80% of all frauds committed. Knowing how those twenty types of fraud are developed, analyzed, and dealt with allows a forensic expert (or a judge) to organize and conduct successful investigations and a company consultant to conduct adequate preventive anti-fraud checks.

Considering the report's findings regarding smaller organizations, which comprise nearly all our country's (Italy) businesses, is necessary. In this case, the ACFE study demonstrates how smaller companies suffer more significant losses than larger organizations and are subject to greater risk because an adequate anti-fraud control system notoriously unprotects them. For instance, it was discovered that small businesses with less than 100 employees had £150,000 as the highest median loss compared to the most prominent organizations (made up of 10,000+ employees), whose highest median loss amounted to £138,000. Although the results seem similar, it is crucial to underline how the impact of such losses is more considerable in smaller organizations (ACFE, 2022, p.29).

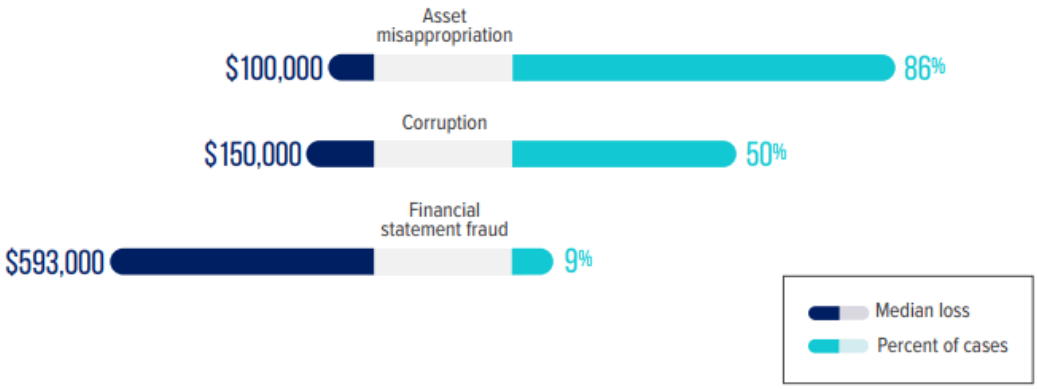
The same analysis can be done with the result of the investigation regarding the distribution of victim organizations based on revenue sizes. The ACFE report shows how the median losses in small organizations amounted to £100,000 and £150,000 in the largest ones, meaning that a small business whose revenue is less than £50 million is going to be having a more significant impact than the larger ones whose income fluctuates around £1 billion or more. (ACFE, 2022, p.30) Similarly, it is interesting to analyze how fraud schemes tend to vary by organization size, showing the public that the corruption schemes are the most frequent in both small (24%) and significant (54%)

organizations, but, moreover, the check and payment tampering scheme is found to a great extent in the small organizations (10%) over the larger ones (8%).

Suppose the so-called "fraud triangle" identifies pressure/incentive, opportunity, and rationalization as the three underlying characteristics of fraudulent behavior. In that case, small businesses face an increase in the second (the opportunity)—the absence of adequate controls and the concentration of considerable powers in the hands of individuals. The former (entrepreneurs), despite having limited resources to prevent and detect corporate fraud, could implement simple anti-fraud policies and risk response procedures capable of significantly reducing their risk exposure with a cost-effective investment to protect their organizations from fraud. Above all, considering the values mentioned above, the judicial system must feel obligated to try to improve its management of investigative work to make it as effective as possible in containing and limiting such a widespread and concerning phenomenon. For instance, small organizations unmistakably face unique challenges in combating fraud, ranging from limited financial resources and smaller staff sizes that necessitate many people performing multiple functions to the high level of trust required to keep operations running and the business growing. Unfortunately, many of the protective anti-fraud controls on which larger organizations rely are not implemented within small businesses.

To get an idea of the frequency and size of these schemes, it is necessary to refer to the most significant American study in the forensic field on the subject of occupational fraud issued every two years: the so-called Report to the Nations on Occupational Fraud and Abuse produced by the ACFE, Association of Certified Fraud Examiners - whose latest version currently available refers to the year 2022. The survey sample, containing

2110 cases of internal fraud occurring in 133 countries, of which 145 just in Western Europe, indicates that among these three types, the most common is that of asset misappropriation - which appeared in 86% of case studies with a loss of $100,000 on average, against 50% of the corruption case, with a loss of $150,000 and 9% of financial statement fraud with an average loss of $593,000 (ACFE, 2022, pp.70-88).



. .

Fig. 8 – "How is occupational fraud committed?" [8]

	Cases	25th percentile	Median (50th)	75th percentile	Mean*
ALL CASES†	**2,046**	**$20,000**	**$117,000**	**$600,000**	**$1,783,000**
Schemes					
Asset misappropriation	1,605	$20,000	$100,000	$500,000	$1,203,000
Noncash	284	$10,000	$78,000	$500,000	$921,000
Billing	281	$20,000	$100,000	$500,000	$852,000
Expense reimbursements	140	$10,000	$40,000	$100,000	$152,000
Skimming	137	$10,000	$50,000	$188,000	$185,000
Check and payment tampering	135	$26,000	$100,000	$500,000	$1,020,000
Cash on hand	129	$5,000	$15,000	$100,000	$131,000
Payroll	117	$10,000	$45,000	$185,000	$201,000
Cash larceny	103	$10,000	$45,000	$389,000	$6,920,000
Register disbursements	25	$5,000	$10,000	$42,000	$33,000
Corruption	906	$25,000	$150,000	$1,000,000	$2,647,000
Financial statement fraud	150	$100,000	$593,000	$6,000,000	$50,482,000

Fig. 9 – Statistical Appendix [9]

[8] Scheme retrieved from page 9 of Association of Certified Fraud Examiners. (2022). "*Report To The Nations On Occupational Fraud And Abuse".* Global fraud study. ACFE.

[9] Statistical appendix retrieved from page 89 of Association of Certified Fraud Examiners. (2022). "*Report To The Nations On Occupational Fraud And Abuse".* Global fraud study. ACFE.

Above all, considering the values mentioned above, the judicial system must feel obligated to try to improve its management of investigative work to make it as effective as possible in containing and limiting such a widespread and concerning phenomenon. For instance, small organizations unmistakably face unique challenges in combating fraud, ranging from limited financial resources and smaller staff sizes that necessitate many people performing multiple functions to the high level of trust required to keep operations running and the business growing. Unfortunately, many of the protective anti-fraud controls on which larger organizations rely are not implemented within small businesses (ACFE, 2022, p.38).

In order to prevent and detect fraud, it is necessary to be familiar with as many fraud schemes as possible. Many believe that the best taxonomy for corporate fraud identity is that used and provided by the Association of Certified Fraud Examiners (ACFE). This classification has now been consolidated over time and includes 51 types of fraud. Indeed, fraudsters are constantly inventing new ways to commit fraud, but it is also true that, in most cases, the activity can be traced back to one of the most common schemes identified by the ACFE. The ACFE taxonomy is also helpful because it collects all possible fraud schemes into three macro categories, which is especially useful for fraud auditors and investigators in their work, as shown in figure 6. The fraud tree model described above ranks these three macro categories into sub-categories and micro categories, assuming a tree's typical structure.

The top three categories of fraud are financial statement fraud, asset misappropriation, and corruption. The first two are mentioned in Statement of Auditing Standards n.99. After defining fraud as intentional acts resulting in material errors in financial statements, these accounting inaccuracies are categorized as fraudulent financial reporting and misappropriation of assets. Each of the three macro categories

identified by the ACFE has its characteristics, allowing for a quick comparison among the three (Singleton et al., 2006).

i. Corruption Scheme

Undue influence is the first component of corruptive fraud, including conflicts of interest, improper gratuities, and economic distortions. When it comes to employment fraud, one or more employees will commit acts that are not in the best interests of the company in order to gain a personal advantage. Employees in the company's purchasing department are the most vulnerable in this regard, as they may buy goods from a specific supplier even though the quality and price of its products are not the best on the market, to receive kickbacks, that is, hidden payments usually taken (in part) from the briber's earnings (AICPA, 2009).

The true leitmotif of corruption schemes is the kickback. As a result, the best way to uncover such schemes is to look for unknown or unexplained financial transactions with some related party (in a broad sense), particularly those addressed to the personal accounts of employees or their family members. When investigating this type of fraud, it is critical to look into potential conflicts of interest, and the problematic areas in companies usually include: large payments made with untraceable methods and "suspicious" payments in corporate accounting books, the payment of intermediaries with ambiguous purposes and motivations or intangible services performed for the company, the receiving or paying off gifts such as travel expenses, the retaining and obtaining of detailed documentation on the substance, purpose, and mechanism of transaction approval, and the checking whether payments were made to facilitate the business (Manning, 2005, p. 39 and Skalak et al., 2012, p. 215).

Personal relationships and payment links appear to play a significant role in this type of investigation. Similarly, documentation and other evidence of receipt of services become critical in determining the presence of an underlying reason (and the correctness of the amount allocated for it). The assignments in this field are known as the valuation of services, and all those payments for consultancy often symbolize the most common impediment: if there is no documentary evidence to prove the professional consultation or the market value assigned to it, proving that it is not a kickback can be difficult (Crumbley et al., 2015, p. 79 and Skalak et al. , 2012, p. 232).

The auction disruption, which consists of manipulating the sales process so that the bid and related winner of the supply/contract/tender, in general, has been secretly pre-determined, is a common element in corruption schemes. There are numerous ways to manipulate an auction, including ensuring that there is only one offer (bid suppression), the creation of other but excessively high offers (complementary bids), and organizing offers in a pre-ordered manner. However, in some cases, the manipulation does not even require the presence of the employee or the internal personality of the company: suppliers, for example, without internal support, may decide to win in turn by always offering higher prices than those of the market in the case of multiple tenders. This is known as bid rotation and falls under external rather than employment fraud (Singleton & Singleton, 2010, p.64).

ii. Asset Misappropriation Scheme

The problem of theft within businesses that deal with money (cash or otherwise), produce easily transportable goods, or build technologies is very relevant. Its treatment must become the key to success for many companies. With any preventative measure that the company may implement, any asset remains vulnerable to theft by employees or

third parties acting alone or colluding with others. To discuss these fraud schemes, it is necessary to first consider how much, in any case. (Skalak et al., 2011, p. 233) The focal point of asset misappropriation schemes is the improper conversion of a corporate asset to personal use: it is thus not necessary for the asset to be stolen, but it is sufficient that it "lends itself" to personal use. Employees at any level may appropriate company money, goods-commodities, or anything else that constitutes the company's assets (obviously, money remains the one with the highest risk).

The ACFE taxonomy divides them into two categories: cash frauds, which involve the misappropriation of financial assets, and non-cash frauds, which involve assets that are not financial. This type of fraud can occur at various stages of the business process, including the revenue cycle (skimming, which conceals a portion of the revenue and does not record it in the accounting books) and the expenditure cycle, but also the production process (with thefts on company inventory) (Pedneault & Rudewicz, 2012, p. 30).

Cash frauds

Regarding cash frauds, globally, cash transactions appear to be decreasing; however, money remains the asset that, for obvious reasons, lends itself best to such actions; as a result, it is the most frequently targeted asset. When we talk about "money," we want to include both cash and bank accounts (especially when the amount in cash is not always perfectly reconciled with the accounting balances). Forensic accounting aims to determine whether money has been kept off the books (so-called off-book cash), such as "slush funds" (Golden et al., 2006, p. 503), because this is the most natural starting point for schemes—more extensive and more complex fraud schemes (all corruption

schemes, for example). As a result, the forensic accountant is constantly looking for indicators that can alert the company to the existence of black funds. Understanding the operation of cash fraud schemes is critical for him (Crumbley et al., 2015, p.43).

This area of asset misappropriation schemes can be divided into three categories, respectively, cash larceny, skimming and fraudulent disbursement. Theft of cash can occur directly from the recipient, at the time they receive it, or at the end of the day from the daily income received. It is typically carried out through the following techniques: falsification of the accounting book, the alteration of documents (receipts), and failure to report receipt of the money (no receipt or invoice is issued) (Wells, 2013, p.91).

The most common form of rationalization is the "loan," while pretending to use them for goods never actually purchased is one of the most popular practices used by scammers. Because of the large amounts of money (usually cash) they generate, many industrial sectors, such as bars, restaurants, and all retail, are more vulnerable to this type of fraud. There are various ways in which an individual can steal money, the main ones including the following: Stealing from petty cash, many businesses have small cash available to employees to ensure that they have cash on hand for minor expenses that are vulnerable to theft. Controls typically delegate responsibility for cash to a single individual, and reconciliations are performed regularly to verify the amount. Secondly, stealing from the bank account: it is critical to have robust internal control over cash receipts, including verifying bank deposits. Bank reconciliations become even more critical as a result: if these checks are not performed, it will not be noticeable that the money in the account has not been reached. Changing documents, such as pay slips or deposit receipts, is sometimes subject to discovery, but if several people collude, everything becomes more complicated for the company (Wells, 2014, p.55).

One of the most common types of embezzlement is "skimming," an English term for stealing a portion of the money received at a specific time of sale. They are all "off the books" fraud schemes, that is, pre-registration of the sale in the victim company's accounts; as a result, no traces are left to be followed - for example - by statutory auditors. They may raise a few red flags25 during the preventive audit checks, but nothing more. These schemes are frequently linked to what is known as "fraudulent sales schemes," such as the manipulation of credits, discounts, and receipts, the intentional under-accounting of sales, or over-shipping. Skimming, in particular, can take place in sales since, due to the employee's implementation of the fraud, sales may go completely unrecorded or be recorded for a lower amount.

To avoid this occurring during the credit verification phase, once this scheme has begun, it needs constant coverage by the scammer, who will be called to make the proper payment in place of a subsequent one. Another occasion for fraud is through credits and discounts, as credits may not appear in the accounting records before being collected by other means, or they may be added by the employee concerning a customer who has already paid.

This fraudulent treatment of credits is also a popular method for creating black funds or paying an employee "off-the-books" following corruption. Lastly, the over-shipping of goods regards cases in which an excess shipment is sent - specifically - and the customer agrees to repay the company employee in a manner unrelated to the accounting books. Another scenario is that the customer, unaware of everything, is led to return the excess goods to the location indicated by the scammer employee, who will direct that load to a location outside the company's control (Skalak et al., 2011, pp. 456-62).

Fraudulent disbursements are the broadest category of money embezzlement of the three. The purchase of goods and services presents an excellent opportunity for those scammers who, by paying suppliers for goods and services that were never received, overpaying them, or even creating fictitious suppliers, manage to get money out of the company while keeping a lawful semblance of it. They can be supported by: The "over-purchase" scheme addresses payments for unnecessary goods or services and, in many cases, unrelated to the business activity or made at a price higher than the market price. Because only the purchasing function is aware of the various supplier offers, it becomes a complicated fraud to detect in the company and could go undetected for a very long time.

The person responsible for the company's fraud will then be "remunerated" directly by the supplier in the wrong way. Fictitious suppliers if the company's internal controls for approving new suppliers

are lax, an employee could commit fraud by adding new ones and assigning them the number of their bank account (or creating a specific round of money with the same objective). Simply entering payment requests to a supplier will suffice to credit the fraudster with the funds (Telpner & Mostek, 2003, p. 136). Tender bidding falsification, especially if there are no specific procedures to follow in the event of a supply contract, excess payments, and embezzlement phenomena aimed at bid-rigging (Singleton & Singleton, 2010, p. 85), may occur (Pedneault & Rudewicz, 2012, p. 30).

This area of fraudulent disbursements is completed by schemes such as double payment of invoices, payment to the wrong supplier or overpayment, and the simple carrying out of personal expenses. It is also worth noting the presence of so-called payroll schemes, all appropriations related to corporate personnel, among the fraudulent payments. Thefts can also result from incorrect payments made to their employees, such as salary overpayment, where, for most employees, the salary is determined by the number of hours worked and the rate per hour. To defraud the company, one of these two must be falsified. Another example is the illicit increase of commissions and bonuses as well as compensation for accidents (usually through the company's insurance) even though the employee is not ill (this subject usually acts in collusion with a doctor). Lastly, there is the possible presence of the so-called "ghost employees," people who do not work but have somehow gotten into the corporate payroll system. In another, more common variant, the same manager inserts additional names to create black funds that can be used for illegal purposes (ACFE, 2011, pp.1525-7).

Non-cash fraud

Concerning non-cash, fraud can be classified as theft or misuse and affect both tangible and intangible assets. Tangible assets, in particular, usually referring to warehouse thefts, which are as common as they are costly for many businesses. These schemes can be implemented using simple behaviors or complex mechanisms to avoid detection. For example, it could be to accurately falsify the records of an inbound shipment or one destined for a client. In some cases, the destination has been changed to a fake warehouse outside the company's control, or the codes of the type of material received have been falsified to buy it at a low price from the company and resell it on their own, making the difference.

The warehouse theft system is nearly infinite, but it always involves two precise files: the warehouse account (in the value of the goods sold or received) and the physical inventory. On the other hand, intangible assets are intellectual property thefts such as trademarks, patent rights, industrial methodologies, trade secrets, research and projects, marketing strategies, and much more. In this case, the risk is even higher, but the damage done is often more significant than one realizes: protecting one's intangible assets, therefore, should always be a priority of management, which is often overlooked (Singleton & Singleton, 2010, pp.92-4).

iii. Financial Statement Fraud Scheme

Accounting fraud schemes are a vast and complex field, and if summarizing fraud schemes of the previous type and those of a corrupt nature in a few lines is difficult, it becomes prohibitive for them. When errors in historical financial information are discovered, a company (usually its auditors) is required to make all budget adjustments. This type of error can result from an unintentional event or from a deliberate intent to defraud; only the latter case manifests itself in the falsification of accounting records or the misapplication of accounting principles in order to achieve the desired economic-financial result.

Weak internal controls, managers' remuneration linked to financial results in the financial statements, or simply the need to appear to the outside world in a situation that is not real are the foundations of employment fraud in the financial statements. Even if it may harm the company, those most affected by fraud in the financial statements are the current shareholders, potential shareholders, investors (even potential investors), creditors, and - in general - all those who rely on the financial statements (Singleton &

Singleton, 2010, pp. 62-5).

Calculating this limit of materiality, that is, the limit at which it is possible to influence the decisions of end users, is neither objective nor straightforward, and usually qualitative and quantitative methods are used, which can be summarized in a kind of "rule of thumb" whose identity is one of the first parts of any statutory auditor's work. It is crucial to underline that these frauds are usually committed by senior management, by mid and lower-level employees, and then, in the least amount of cases, by organized crime (Wells, 2014, pp. 273-6).

Financial statement fraud is classified into two types: financial and non-financial. Although the most common scheme is based on increased revenue, the ACFE highlights five schemes based on time differences, delayed debts, fictitious revenues, inadequate disclosure of income and expenses, and improper corporate asset evaluation. Regarding time differences, the shift in time is used to boost or decrease the revenue accounted for in the current year; for instance; a shipment could be intentionally made in a manner that results in lengthy transit, making the customer sign the sales agreement before the goods are delivered (Zack, 2013, pp. 91-2). Following, delayed debts are postponed to reduce the ones of the current fiscal year (usually inserted into the first month of the following fiscal year) (Ibid, pp. 93-94). Fictitious revenues are ad hoc sales made with natural or fictitious customers. There will be increased revenues and profits at the end of the year and overvalued assets (Ibid, pp. 33-36). Furthermore, by inadequate disclosure of income and expenses, there will be false and exaggerated earnings, as any insufficient assertion can be both the source of the object of fraud (Ibid, pp. 187-96). Lastly, there is improper corporate asset evaluation where individuals tend to focus on assets with complicated valuations, such as complex financial instruments, real estate, or securitized assets.

All revenue recognition schemes attempt to increase the amount of revenue recognized or to accelerate recognition over time: for example, they can be found in the sales balance sheet within the reference period. However, according to accounting principles, they should be recognized in the following year because the conditions underlying the sale have not yet been completed. A company may complete the production of a good, but the customer will not be ready to receive it in the reference year: to expedite the sale, it may be shipped to a third party, who will record the sales in the balance sheet. To do so, however, the customer would have to assume the asset's title, risks, charges, and ownership rights - which is often not the case. Another method of revenue recognition fraud could be to treat a retailer as if he were an end customer and, as a result, not adequately consider agreements for the return of unsold goods, which are only aimed at completing budgeted sales in the current year (Lundelius, 2011).

Expenses and costs can be manipulated through illegal deferrals, as with revenues, but also through improper capitalization of expenses, long-term contracts with underestimated costs, exchange rates following impairment that are not implemented, manipulation of exchanges, unsupported supplier discounts, and - in general - improper use of the balance sheet account in "invoices to be received" (Zack, 2013, pp. 263-5).

Overall, the ACFE presented the following two methods: fund manipulation and all activities not reported in the accounting books. The funds to be allocated and set aside refer to advances for future outflows or losses, but certain conditions must be met before a fund can be recorded in the financial statements (such as a reasonable estimate of the amount and adequate information on the timing). An investment received but not accounted for will inevitably lead to investors not fully understanding corporate debts

(ACFE, 2011, pp. 4520-2).

Because of the subjectivity of the nature of the funds, it remains a very vulnerable post to abuse; additionally, the creation of fictitious funds to reduce the tax burden and "free them" in more difficult times is a practice that has been abused over time. An investment received but not accounted for will inevitably lead to investors not fully understanding corporate debts: Enron was the case that helped bring to national attention the real possibility that any company can have transactions not recorded in the accounting books in order to confuse its investors about the true economic nature of the transactions carried out.

The Enron Scandal

The Enron scandal is one of the most known frauds globally and decisively one of the most discussed and studied today. Founded in Houston, Texas, in 1985, Enron Corporation was a business operating in the energy sector, and during those years, the American gas market was going through a deregulation phase. The Federal Energy Regulation Commission emitted an order (436) that separated the acquisition and the delivery of gas into two diverse processes, and due to this regulation, companies in the energy sector had switched from providing bundled gas purchases to simply acting as intermediaries between the ones producing and the ones acquiring the gas. Furthermore, this gas deregulation increased users' exposure to the natural volatility of the prices. Thanks to this complication of tariff planning, Enron Corporation expanded into new markets that were much less regulated (Fusaro & Ross, 2002).

During those years, Enron began to employ the mark-to-market (MTM) method, which allows for assets to be recorded in financial statements at fair value, rather than the traditional methods with used book values. Nevertheless, this method's main

problem is that fair value is frequently hard to determine since it is closely linked to various market conditions. Enron had a significant discrepancy between the actual and the declared cash flows (CFI, 2020). To make matters worse, the company used Special Purpose Entities (SPEs) to circumvent and hide its financial misdoing and losses. By transferring assets and liabilities through these entities, Enron could hide its losses from the company's balance sheets and balance out any imbalances. Nevertheless, this brought the company into a vicious cycle where they would augment their debt and hide the losses through these "shell companies." By reporting these losses in the SPEs and using the MTM method, it was almost impossible for financial analysts to even link these back to the company (Ibid, 2020).

However, in 1999 the committee in charge of ensuring that the accounting standards were met by Enron (the Corporate Control and Compliance Committee) discovered some severe issues. Specifically, nine of the company's accounting practices were classified as "highly risky," a report that led to the collapse of the Enron empire. Inevitably, as a result of the public outcry over the report, the company started undergoing a decline, and in 2001 the real downturn began as the Securities and Exchange Commission (SEC) started launching a series of investigations into the company. As soon as these financial investigations' findings went public, the company's stock began to plummet, and by the end of 2001, the price went from $90 per share to $0,26 per share. At the end of 2001, the famous and seventh-largest company in the United States collapsed and went bankrupt, resulting in the second-largest bankruptcy case in the history of the country. More than ten congressional committees were investigating the company, and the actual extent of the damages caused by Enron only to its stakeholders is still unknown (Petrick & Scherer, 2003, p. 38).

Inevitably in October 2002, the Securities and Exchange Commission filed a civil

enforcement action against the company's CFO, Andrew S. Fastow (ACFE, 2011, pp. 1314-15). The main parties who suffered from this bankruptcy were employees, investors, and the. The employees received one hour to pack everything and leave the company, and the investors lost thousands of dollars of investments (Mohd, 2020, pp. 5-8). Thinking back, a more thorough examination of the company's investment cycle would almost certainly have revealed this hidden structure, allowing the gaps in the American giant's accounting records to be identified much earlier, and this examination today would have been conducted by forensic accounting experts.

The lack of independence between the company, Enron, and Arthur Andersen, the auditor, was one of the most shocking aspects of this fraud. Auditors are required to be independent of their clients, which lowers the likelihood of audit failure. They were not independent because Arthur Andersen continuously did non-audit work for the company (such as tax returns and consulting). Enron managed to earn more money from non-audit work than they did from audit work. When non-audit fees account for a sizable portion of an auditor's income from an audit client, the auditor may be tempted to overlook an enterprise's 'aggressive' accounting to keep the client's non-audit business (Barrett, 2002, pp. 16-20). The discovery of this lack of independence resulted in significant changes to generally accepted auditing standards and the way auditors are monitored. Non-audit services provided by CPA firms to audit clients are now illegal.

Worldcom

Following the American giant Enron, another American Corporate filed for bankruptcy on July 21, 2002, when Worldcom, the telecommunications giant, resorted to Chapter 11 of the United States bankruptcy law (Schroeder et al., 2020). It is arguably the largest accounting fraud in history. It appears to be the largest corporate

bankruptcy ever. This scandal exposed the true problem that had reigned in United States business and government up until that point, namely greed and corruption. Inevitably, this decreed a strong mistrust of investors and consumers in global markets, resulting in a series of bankruptcies of various American corporations; we could call it a true domino effect.

The company, WorldCom Inc., started as a small provider of long-distance phone service. During the 1990s, the company grew rapidly through aggressive acquisitions of other companies that dealt with telecommunications. In 1998 the company took over MCI Communications, which allowed it to become the second-largest telecommunications company in the world. Following this, the company also acquired CompuServe, UUNet, and the America Online data network, turning WorldCom into one of the giant internet providers globally. In 2001 WorldCom's revenues were around $40 billion, more than any other company in the United States. Nevertheless, in the 1990s, there was a great oversupply of telecommunications capacity, meaning that the company had to compete with other providers for bandwidth and immediately rushed to build new facilities and fiber optics networks. However, the company did not succeed in growing faster as the dot-com boom ended and the economy of the country (and the rest of the world) crashed in the early 2000s leading to a recession. The revenues fell short, and the debts taken on finance merger, and acquisition investments never paid off (Lyke & Jikling, 2002 and Barrett, 2002, pp. 16-20).

This rapid downturn began in 1999 and continued at a rapid pace until May 2002, when the company was led by Ebbers, who held the positions of (CEO), Scott Sullivan (CFO), David Mayers (Controller), and Buford Yates (Accounting Director General), all of whom used fraudulent accounting methods to mask diminishing earnings and keep the price of Worldcom's Nasdaq-listed shares always high. Worldcom was a real

accounting swindle (for a six-fold higher value than Enron), with 3.8 billion operating expenses incorrectly accounted for as capital expenditure, inflating profits and misleading market investors. These expenses were purposefully spread across several capital items to manipulate profits and hide reality.

WorldCom is undoubtedly one of the most famous types of financial statement manipulation frauds by capitalizing expenditures for "line costs" (Crain et al., 2016, pp. 390) which are fees paid by the company to third-party telecommunications network providers for access to their networks. According to GAAP, these fees should be recognized as an expense rather than capitalized. Beginning in 2001, however, WorldCom's management documented line costs in the real estate, plant, and equipment account rather than the expense account. Thanks to this reclassification, the forecast consensus was met by analysts even though the company was understating both earnings and expenses. WorldCom seniority knew that auditors would perform the usual analytical procedures on all the accounts in the financial statements (equipment, plant, and property) and because the company was undergoing a decline in those acquisitions, they knew that the auditors would not perform a full analysis of the line costs as they were going to be similar to the ones of the previous years (Ibid, p. 391).

Internal auditors are the first line of defense against accounting errors (incorrect classifications made with no intent to deceive) and financial fraud (knowingly false classifications made with the intent to deceive). One question about WorldCom is why it took more than a year for the company's internal auditors to discover the misclassification given the number of costs capitalized (almost $750 million per quarter) and the effect on net income and assets and this fraud scheme could have been caught sooner. One of the questions regarding this fraudulent behavior could have been

asked to Arthur Andersen (the company's employed auditing firm), who stated that he had not been notified that the "line costs" were being capitalized as irrelevant and blamed Sullivan (the company's CFO) for the discrepancy (Wisner & Brown, 2015). Nevertheless, Andersen should have paid more attention to the company's instability during those years as Worldcom's financial condition was extremely precarious and, therefore, should have adopted aggressive accounting practices. Overall, the validity of any statement that came out of Andersen was questioned globally as the firm had already been involved and even convicted in several other fraud cases, most knowingly the case of Enron. WorldCom filed for bankruptcy in 2002, the third largest bankruptcy in the United States. as although the company had reported over $100 billion in assets, it also owned over $40 billion in debt (Lyke & Jikling, 2002).

iv. Examples of famous schemes

i. Affinity scheme

Affinity fraud refers to various scams committed on a group of people who are related explicitly by race, religious background, profession, family, sex, or age. The person or people who perpetuate affinity fraud take advantage of these connections and, using the commonalities of a specific group, create a pattern that is most appealing to that group. The criminal's ultimate goal is to steal money from the participants, an unfortunate and common occurrence in many parts of the world.

There are different types of affinity fraud. For example, a criminal may target the families of people who died in the armed forces. He could then solicit donations to include all their names in the name of a monument that will never be built. This affinity fraud has happened frequently in the United States, especially after or during the wars. It is one of the worst frauds because it deliberately exploits the suffering of these

people. It is crucial to underline that in order for this scheme to work, there needs to be an emotional side to the request for an investment; matter of fact, the fraudsters will use this emotional side to play on the feelings of individuals who want to help to fund for a good cause, such as a remembrance monument (Perri & Brody, 2011, pp. 34-5).

In his work (2013), Blois argues that affinity fraud is more common than most people realize and underlines how it is especially so for two reasons. First, many frauds, such as the $33 million fraud committed by an Amish member against his co-religionists, receive little media attention because, while the losses for the individuals involved are often significant, the total amount involved is relatively small. The author's second reason is that many victims do not pursue or make their involvement public due to some form of reluctance as if they were refusing to accept that they had been trapped in this fraud. Furthermore, there is a general overall embarrassment and desire to defend the reputation of their affinity group. The most well-known example of affinity fraud schemes is, indeed, the Ponzi scheme.

Ponzi Scheme

Ponzi schemes, named after the Boston scammer Charles Ponzi, who invented a financial arrangement that failed in 1920, are a type of financial fraud in which participants are compensated with money placed by subsequent subscribers rather than real profits from investments or commercial activities. They generally lure savers into their web by promising higher returns than any legitimate business. To remunerate members, the growth rate of new inflows must be exponential, and the system will inevitably fail when fund requirements exceed new inflows. This combination of fraudsters who steal, together with the promise of such great money returns, unequivocally leads to the scheme collapsing. Most members then lose their

investments, even if the former, including the founders, can benefit from high yields or exceptional annuities if they withdraw on time (Crain et al., 2016, p. 283).

Ponzi schemes are costly for most participants and divert savings away from productive investment. If no one opposes them, they will grow disproportionately, causing significant economic and institutional damage, undermining trust in financial institutions and regulators, and putting a strain on the budget in case of a bailout. Their demise can even cause economic and social instability. Ponzi fraud schemes usually involve two main phases: the recruitment phase and the investment phase: the earlier of the two is the most expensive for investors. The recruitment phase involves the creation of a false or misleading profile of the company or individual and using deceptive tactics to get people to invest in the scheme. The investment phase is when the money is invested in the company or individual and when the person promising returns makes their promises, usually over time, about the rate of return, the time frame, and other essential details, such as the company's financial strength and the amount of money that will be invested in the company. During this phase, the promoters usually claim that the gains from the investment will be more significant than the investment costs, creating a pyramid scheme that can reach millions of people (Surendranath & Mark, 2011, pp. 5-6).

For the Ponzi scheme to work, it is crucial to underline the importance and role that trust plays in this fraud. The role of trust in all types of fraud schemes is exciting as, in almost, all corporate fraud cases, an employee of the business commits the fraudulent act, usually also covering the highest positions; hence, a person that is usually very trusted by the company. However, as Carey and Webb (2017, p. 590) explain in their article, trust is essential for this Ponzi scheme to work. The schemer needs to create and build a solid trust with plausible investors, a trust that goes well beyond the investment

of money. Usually, an individual would be keener in lending money or spending money for someone they know, someone that resembles them, meaning that the schemer does not only have to promise significant incomes but also put himself in the position of the investor. The bigger the trust, the greater the amount of money. This building of trust is essential for the investor to not continuously worry or ask for updates and news regarding the investment made without due diligence. The worst part about this pyramid scheme is that usually, the frauded investor becomes the schemer by proposing this great new income idea to friends and family members, completely unaware of the consequences (Ibid, p. 592).

Furthermore, because these pyramid schemes usually start without legally registered businesses, the regulators, whose role is to ensure that these frauds do not occur, have a hard time detecting these schemes before some damage has already been done. Putting a stop to Ponzi schemes when they are still at the beginning is extremely difficult as the schemers work hard and study the situation well while taking the proper steps to ensure that no information is leaked. The initially employed individuals are men of trust, employees that will almost entirely for sure not denounce the scheme after being done with the fraud. The most successful Ponzi frauds have usually also involved connections with high-ranked investors and politicians who would make it less likely for any antifraud commission (such as the Security and Exchange Commission in the United States) for the fraud to be unveiled (Khuzami & Walsh, 2009). Lastly, when the Ponzi scheme is finally discovered by the assigned government regulators of the specific country, the main perpetrator receives a lawsuit, and an agent is then appointed to try and recover as much of the investments possible and ensure that the perpetrator makes the proper repayments to the creditors as well as the investors. However, the agent will usually check whether other players (such as the bank) ignore the obvious red flags and

will take legal action against them. Any entity or even individual involved in the scheme through the investment of money without applying due diligence can be prosecuted (Sauer, 2010). Nevertheless, research such as the “Relational models theory” (Fiske, 2004) has shown that the mere exploitation of trust from schemers in order to acquire financial gains in the form of fraudulent investments is insufficient in explaining the scheme’s long-term success.

ii. Advance fee fraud

Because of the anonymity of the networks, many different types of scams and fraud have emerged. Hackers use the Internet's speed, the existence of social networks, and email to carry out their crimes. The advance payment scam is one of the many ways people are duped online. This type of fraud is intended to appear as a legitimate and appealing transaction, making it difficult for the victim to refuse. As the name suggests, an "advance fee" down payment constitutes so-called advance fee fraud. This fee must be paid in order for a transaction to be completed. This fraud scheme involves tricking individuals (who become victims of fraud) into advancing small sums of funds, hoping to gain an advantage in the transaction and a significant gain overall. Like most online scams today, advance payment scams employ classic social engineering tactics in which scammers persuade their victims to make an advance payment in exchange for a service, item, or loan. This type of fraud includes the provision of investment opportunities, the sale of services and goods, the winning of the local lottery, and even the unbelievable discovery of money. (Fokouh, 2009, pp. 67-72).

According to the Federal Bureau of Investigation (FBI), an advance payment scam occurs when a victim pays someone money in exchange for something of value that they never receive. To entice their victims, these scammers usually create very

appealing offers. The strange thing about advance payment scams is that they have been around for a long time; they were previously known as the 419th scam or the Nigerian Prince mail fraud. The Nigerian prince scam is the most common advance fee fraud scheme involving a non-existent Nigerian prince. He seeks an investor to aid him in transferring money (usually around millions or even tens of millions) from his country into the victim's country by promising a share of the amount. As Wagner (2004) explains, in the early 2000s, there was an estimated daily loss of $1 million in the United States alone from these scams. This fraud originated in the 1970s; however, the scheme involved the usage of postage mail and telephone calls, making it already highly profitable at the time. The Internet explosion in the 1990s has made it even easier to carry out these types of scams and attract more and more victims into the scheme (Webster & Drew, 2017, p. 72).

This con is based on the story of the "Spanish prisoner card," which was first used more than a century ago. At the time, the scammers sent letters to various people in business claiming that a wealthy individual was imprisoned and that, in exchange for a portion of his fortune, he requested assistance in the form of a contribution that his victims would have to pay. Once the "contribution" was paid, the prisoner's identity was never revealed, and there was no shared wealth. The scheme ends when the fraudster receives the money and simply disappears (Alli et al., 2018, p. 78).

iii. Pump and dump scheme

The so-called pump and dump scheme is a securities scam usually involving stocks. Scammers create false advertisements about a stock to generate interest, and once investors start buying shares, the share price rises. It usually involves two brokers who continuously trade the stock at higher prices and sell the stock shares to another investor. Usually, the victim, after the purchase of the shares, discovers that they have

fallen in value at high speed (Manning, 2012, p. 366). Essentially, when the price reaches a certain point, the scammers behind the false advertising sell all their shares. This occurrence causes the stock price to plummet, leaving new investors with the stock.

Inevitably, the internet has been used by fraudsters to solicit investors for decades, especially since, nowadays, the creation of a natural and legal-looking website or e-mail has become simple for even the least knowledgeable of individuals. Forensic accountants now have to deal with the so-called "cyber crashes" and the ever-changing ways of exchanging goods and services through different types of payments online. Cryptocurrency fans view Bitcoin, Ethereum, and Dogecoin as the future of money for the world. The underlying blockchain technology allows cryptocurrencies to work by creating a digital ledger that records transactions, which would create a more secure form of currency. Nevertheless, where money can be made, scammers are not far behind. (ACFE, 2011, p. 2424). Cryptocurrency pump-and-dump schemes are designed to take advantage of people while making money for scammers. They typically involve influencers receiving financial incentives for telling people to buy a particular digital currency to increase its value. Once the value increases, scammers and influencers sell their coins and pocket the profits, while everyone else sees their investments lose value.

The Security and Exchange Commission deals with the continuous increase of the pump and dump schemes which tend to involve newer means of communication every day. There is a mixture of e-mails and message board postings on various websites where fake analysts who are deemed as reputable are posting "groundbreaking" information regarding a particular cryptocurrency, pushing not-so-knowledgable individuals into investing in these companies leading to the victim losing the funds while the fake analyst profits off of them and disappears. The Internet Fraud Complaint

Center of the United States is filled daily with new websites that are fake and soliciting victims into investing in fake stocks (Crumbley et al., 2015, p. 919).

The most famous case of the pump and dump scheme has to be the one involving Jordan Belfort, the internationally recognized "stockbroker" depicted in the movie "The Wolf of Wall Street." In 1987 this stockbroker who worked for a small firm specializing in penny stocks was successful enough to be capable of making large amounts of money through the sale of the stocks mentioned above. Later on, Belfort opened Stratton Oakmont, his firm in the 1990s, where there would be brokers increasing the price of stocks so that then Belfort and his partners would suddenly retrieve or, better, "cash-out" all the money, causing a plummet in the value of the sold stocks. After years of this fraudulent pump-and-dump scheme, in 1998, he was indicted for money laundering and securities fraud (Kayvon, 2021, pp. 38-42).

iv. Money-laundering scheme

Money laundering schemes regard the process of introducing illegally acquired funds into the financial system. The expert money launderer's goal is to make it appear as if the laundered funds came from legitimate sources. This type of scheme is a far more pervasive crime than most people realize; it could be stated that many crimes, from embezzlement to drug trafficking, often include money laundering.

In simple terms, money laundering is giving a legal appearance to a product or service derived from drug trafficking and all crimes typified in each country's criminal code, including administrative corruption, tax evasion, and corporate fraud. Money laundering is widely regarded in many countries as a legal activity. It is perhaps the most complex criminal activity, specialized, difficult to detect and verify, and one of the most profitable sources of revenue for criminal organizations, however, although money has

been laundered worldwide for a long time, it is only since the 1920s that some authorities have begun to address the issue, albeit cautiously (Crain et al., 2016, pp. 266-280).

The profit motive that sometimes guides criminal activity has demanded that delinquency design of financial and economic structures through which it is possible to channel the resources obtained due to their illicit activities. These monetary resources then flow through various economic sectors. Via the development of commercial and financial activities and corporations, an appearance of legality is created. This false appearance leads to monetary gains for the perpetrators and their organized crime association since these products are not considered instruments or effects of criminal activity. This cycle inevitably leads to the enlargement of the criminal activity sphere.

Without a doubt, money laundering carries severe penalties, where each money-laundering transaction can result in a separate twenty-year prison sentence. Furthermore, any funds associated with money laundering are forfeited. In many cases, fraud schemes involve many transactions subject to money-laundering penalties. The money-laundering procedure consists of three steps: placement, layering, and integration. The first step is "placement," which entails depositing the illegally obtained funds into a financial institution to ensure that no suspicious figures arise or appear. Second, the "layering" step entails moving money from one account to another so that it cannot be traced back to the first deposit made during the placement step. Finally, integration is concerned with finding ways to make the available funds for the use of the money launderer while avoiding suspicion (Pedneault & Rudewicz, 2012, pp. 130- 140).

There are various placement techniques used by perpetrators, the most popular including "smurfing", a widely used technique. It entails dividing large sums of money into smaller deposits of less than $10,000 each since financial institutions must report

cash deposits greater than $10,000 to the federal government. Because of this limit, smurfing is unappealing to drug traffickers or others looking to launder millions of dollars. The currency structure method entails the money launderer exchanging many prepaid debit cards or negotiable instruments (such as money orders) for illegal (or occasionally legal) goods or services. One example is swapping illegal drugs or diamonds (purchased with cash) for debit cards. Furthermore, the front companies method is famous for groups of criminals as it involves the construction of a legal business and depositing the illegally obtained cash from a legitimate business. Lastly, the corrupt bank technique is where money launderers have sometimes been known to buy a bank, establish their bank, or bribe officials in a current bank. This method is most efficient in countries with comparatively high levels of corruption and limited economic oversight (Crain et al., 2016, pp. 266- 280).

There are even more layering techniques, such as informal value transfer systems (IVTSs), which is a method for money launderers to transfer funds from one location to another, even across international borders, usually through means such as the famous Western Union. Another popular example of layering is using trusts. In certain countries, individuals are allowed to have anonymous trusts used to transfer money without creating any trace of the connection between the two parties.

There is also the use of off-shore accounts, as banks in certain countries have “loopholes” in their laws, allowing money launderers to move money as much as they would like without their country knowing about it. Another technique is through bearer stock certificates, where particular shell companies will help the launderer move money in and out of the organization without it being traceable to the government and sometimes even the organization’s owners. There is also the usage of walking accounts, where the funds are connected from one location to the other in case of quick removal of

evidence during a possible legal inquiry. Lastly, financial intermediaries are very commonly used; these individuals are usually security brokers or connected to an insurance company (Ibid).

The last step mentioned in the money laundering process is that of integration, and the various techniques include using offshore debit and credit cards (usually from a foreign country), offshore consulting loans and fees, meaning that hefty "consulting" fees are paid to the money launderer by an offshore business owned by the same. Furthermore, there is the prevalent technique of gambling, as well as scam transactions and the so-called "under-the-table" cash, which usually takes place around real estate and yacht sales, where some of the money is received in cash and, therefore, not invoiced. Other techniques include scam stock purchases, where the money launderer places long and short commands for the same amount of security shares, leading to one position gaining and the other losing. The loss is then "tear up" by the stock broker, leaving only the gain. The money launderer pays the broker cash for the gain and a "fee" for the deceitful service. This leaves the money launderer with finances on account from which to draw. Lastly, using a legitimate business is where the launderer sends money to a business under his control and then draws from it for personal benefits. It is important to also mention that today there is also a rise in bitcoin money laundering and other types of digital e-currency transactions. As explained by Crumbley et al. (2015), launderers have found methods of transferring bitcoins to others who are willing to use them on websites such as Agora for the illegal acquisition of guns, drugs and other illegal items.

To combat money laundering there is the Financial Action Task Force on Money Laundering (FATF) which continuously publishes standards, recommendations and laws for the thirty-five member countries. The Recommendations also address the role of Financial Intelligence Units (FIUs) at the national level and the significance of their

international cooperation processes. The rules include a general requirement for the FIU to be as collaborative as conceivable with foreign counterparties, with refusal limited to a few unavoidable cases.

In the European Union, the anti-money laundering dedication began in the early 1990s and has been represented in five Directives and various other measures over the years. The current Fifth Directive (EU) 2018/843 modifies the European Union regulatory regime in some particular places, completing the indicators presented by the Fourth Directive (EU) 2015/849. The Fourth and Fifth Anti-Money Laundering Directives strengthen Member States' prevention systems per the FATF's 2012 Recommendations and improve the risk-based strategy, which is a fundamental criterion for adapting preventive measures and checks. More specifically, in Italy, the anti-money laundering legislative framework currently consists of Legislative Decree 231/2007, as recently revised by Legislative Decree 125/2019, and the corresponding implementing provisions issued by the Ministry of Economy and Finance, the Financial Intelligence Unit for Italy, and the sector supervisory authorities (Banca d'Italia, 2022).

v. Fraud investigation cycle

In order to understand the whole fraud process, authors have referred to the organization and implementation of the fraud from the fraudster as well as the reimbursement and solution to the damages as the fraud cycle. In this cycle, one can find all the work and information required to conduct an investigation. Undoubtedly, from an organizational standpoint, fraud appears to be one of the most serious risks that any company must face, as well as one of the most difficult systems to implement:

developing a "system" capable of preventing or even simply carrying out an effective detection is extremely difficult, even though it could be stated that it should be the primary responsibility of all management. Implementing a framework is extremely difficult because no two frauds are ever the same, even if the schemes used (as mentioned previously) are the same. As was already shown, the Association of Certified Fraud Examiners even outlined as many as 49 different types of schemes. However, such schemes work mainly as a theoretical contribution to a plausible fraud investigation. Nevertheless, no corporate fraud is ever committed perfectly. There are always ways for fraud auditors and later forensic accountants to discover key elements that can bring out the whole situation (Singleton & Singleton, 2010, pp. 7-12).

Throughout the years, there has been a rise in the creation of diverse managing corporate risk approaches, especially by assuring that a serious and appropriate system of corporate governance exists. The whole point of corporate governance is to set and monitor the company's objectives, policies, accountability and performance to ensure that all the attitudes and regulations implemented will not allow for any form of creation or even tolerance of fraud. The importance of corporate governance lies within the communication and implementation of corporate policies, even though, as of today, total and complete fraud prevention are impossible (Skalak et al., 2011, pp. 18-20).

Fig. 10 – Fraud deterrence cycle[10]

For instance, in "A guide to forensic accounting investigation" (Golden et al., 2006, pp. 13-20), the authors depict a so-called "Fraud deterrence cycle". This cycle is described as interactive and takes place over time. The four major components described by the authors are the implementation of corporate governance, the implementation of transaction-level control procedures, also known as the internal accounting controls system, audit examinations conducted in the past to examine governance and control processes and the investigation and resolution of suspected or alleged problems. The first component, corporate governance, has already been mentioned. Regarding transaction-level control procedures, they are financial and accounting controls created to guarantee that only legitimate, authorized. Valid transactions occur, as well as to protect company assets from loss from theft or other illicit practices. Following audit procedures conducted in the past, the authors explain how such retrospective investigations can aid in detecting criminal procedures before they become even more harmful to the company. Forensic accountants usually conduct

[10] The fraud deterrence cycle scheme taken from page 13 Golden, Thomas W, Steven L Skalak, Mona M Clayton, and Jessica S Pill. (2006). "*A Guide to Forensic Accounting Investigation*. 2." Vol. 2. John Wiley & Sons inc.

these procedures, and they help form a link to fraud tolerance communication and safeguarding the organization's welfare. Something that may be seen as innocent in a few cases could prove extremely dangerous in aggregate forms. Last but not least, investigative measures eventually led to the creation of the company's control policy based on the findings. These investigations lead to actions that are proportionate to the size and gravity of the impropriety or fraud, whether it is discovered to be a minor offence of corporate rules or a major system to create fraudulent income statements or misappropriate substantial assets (Ibid, 2006).

Nevertheless, the development of corporate ethics programs, the communication to the employers regarding the company's approach to fraud, the training on methods of recognizing frauds, the monitoring of all internal controls and corporate activities and the development of a detection system based at least on red flags, have decreased the number of frauds committed daily. Prevention is thus the best weapon for avoiding being a victim and the enormous costs of an investigation; however, this will never eliminate the risk.

The detection

The fraud investigation framework identifies a specific moment that marks the start of any fraud investigation as planning and organization: the moment of emergence. It may appear insignificant, but a fraud that does not manifest itself in any way is a mechanism that cannot be stopped and causes the victim (usually a company, competitors, or shareholders) to lose money without even realizing it.

As a result, it is clear what the emergence mechanism means: it is the method by which the fraud is discovered. If we were robbed while on tour in the city centre, we

might not notice it immediately. It might not be until we go to buy a coffee that we realize we have been robbed: that is when the illicit fact emerges, and it is at that point that we must decide what to do, such as whether to call the police to report the theft or not. The company, aware that it is a constant target for fraud, can try to implement various emergence mechanisms to ensure that if fraud is perpetrated against it, it emerges quickly and has minor consequences. The ACFE (2022) has updated the frequency of emergence mechanisms for the initial detection of occupational fraud in its Report to the Nations. Its research has shown that the so-called "tips" (especially anonymous ones) are the major method for case scenarios of occupational fraud (and this has been true since 2002, the year of the first research carried out by the American Association).

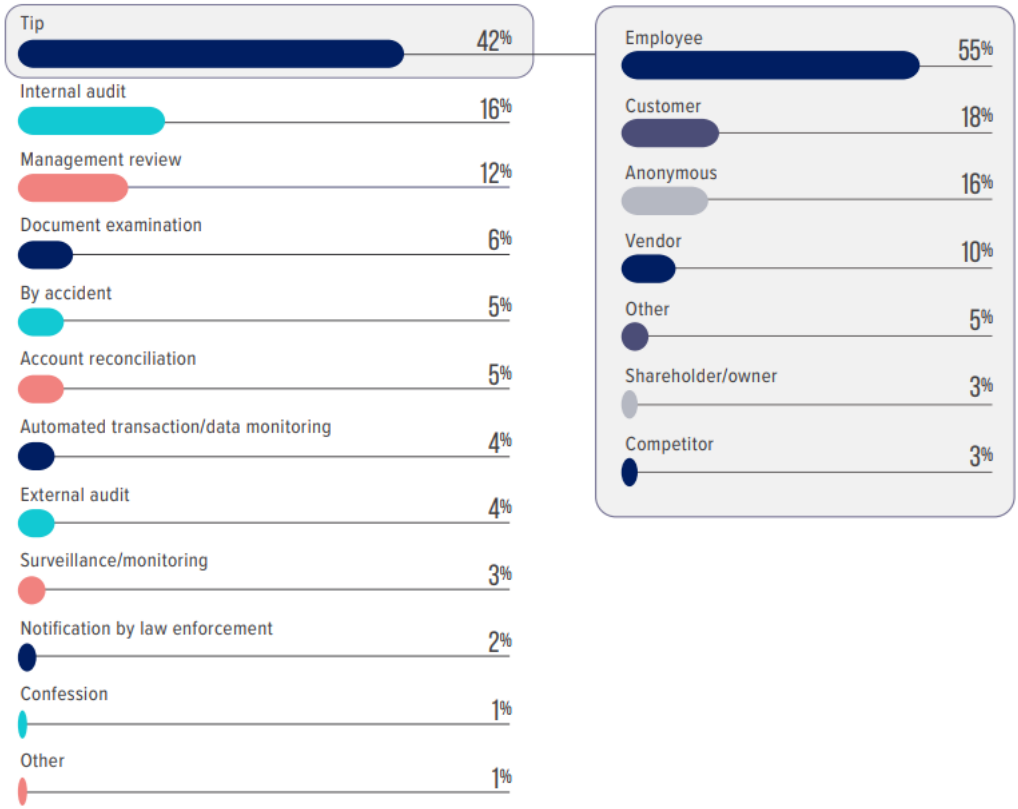


Fig. 11- How is occupational fraud initially detected – Who reports occupational fraud? [11]

[11] Both schemes are retrieved from page 22 of Association of Certified Fraud Examiners. (2022). "Report To The Nations On Occupational Fraud And Abuse". Global fraud study. ACFE.

In the figure is shown how the fraud is initially detected and, in order of probability, it is due to: tip, internal audit, management review, document examination, by accident, account reconciliation, automated transaction/data monitoring, external audit, surveillance/monitoring, notification by law enforcement, confession and “other”. The main detection method is due to tip lines which are all those methods and mechanisms provided by the organization in order to allow the insider the possibility to denounce any form of suspicious activities. There can be various ways in which a suspect of fraudulent activity occurs, however, the so-called whistleblower method or just anonymous online modules are the ones that work best. According to this graph, 42% of the initial detections and thanks to tip lines and, accordingly, by looking at the figure adjacent to the scheme, in 55% of the cases the suspicious activity is reported by another employer (18% of the times by customers and 16% anonymously).

Right after tip lines there is the use of internal audit, however, the difference between tip lines and actual preventative methods is colossal as internal audit only accounts for 16% of the initial detections. This is extremely interesting because internal audit, as the protagonist of the entire company's internal control system, has the task of ensuring effective business management, yes, of looking after company procedures by directing them in the direction of efficient organization, but above all, of establishing a good and effective system of prevention and control through systems of fraud indicators, all factors that would lead one to believe they should be at the very top of the graph.

Management review is found at 12% as in addition to an internal audit, there are various forms of control in company procedures, particularly in activities with a high risk of fraud. For instance, an administrator supervising financial income and expenses could thus see suspicious activities emerge during normal control activities. Following,

there is document examination in only 6% of the cases, meaning that, according to this ACFE research, the reviews performed by internal controls lead to fraud detection only in a small percentage of cases. Furthermore, there is detection by accident, meaning that in 5% of the cases, fraud is detected due to the incapacity of perpetrators to cover their tracks when committing illicit activities adequately. Moreover, in 5% of the cases, fraud is detected during the reconciliation of accounting balances with actual balances derived from the account statement. At only 4%, there is the detection from automated transaction/data monitoring, which is the ability of the company's analytics platform to detect relevant insights, trends and oddities and automatically send what has been detected to specific employers.

The external audit also detects 4% of occupational fraud, and that could mainly be due to the statutory auditor who suffers from the nature of its procedures that are designed for other purposes, mainly the presence of significant errors and the resulting difficulty in discovering illegal activity while following its procedures in an impeccable manner revision. While professional scepticism can be very useful, the importance and type of checks that must be performed work against it, showing how a traditional statutory auditor differs from the figure of the forensic auditor, who considers the risk of errors in light of existing organizational controls, implementing techniques suggested by the three factors of the so-called "fraud triangle". Detection by surveillance/monitoring, meaning the presence of video surveillance systems on company premises or the presence of departments dedicated to detecting fraud by continuously monitoring transactions and processes in large companies, is at 3%. The notification by law enforcement is only at 2%. It is the most expensive detection technique for the organization as it could not intercept it on its own, leading to a third-party complaint and the police launching an investigation against the company. The results of the ACFE

research bring to light the importance and critical priority that fraud investigators should bring to the implementation of efficient processes aimed at soliciting and thoroughly evaluating tips (ACFE, 2022, p. 19).

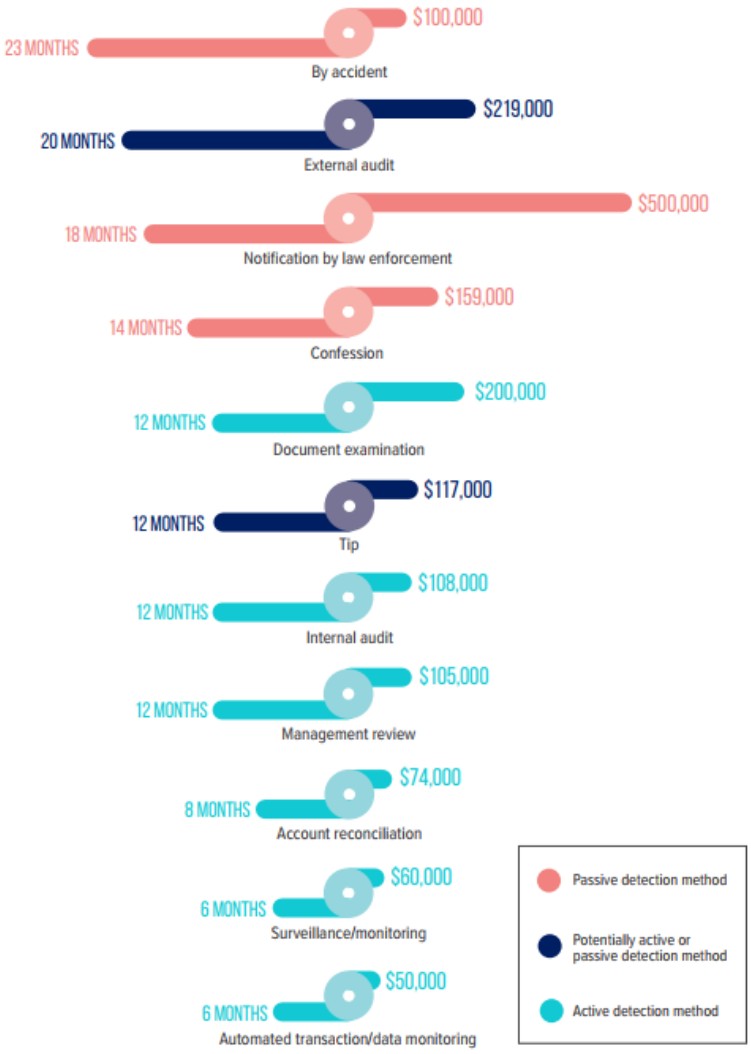


Fig.12 - How does detection method relate to fraud loss and duration?[12]

Furthermore, from the figure above regarding the ACFE research on how detection methods relate to losses, it is clear that certain practices are much more effective than

[12] Figure retrieved on page 23 (Ibid)

others. The data in this figure shows that when fraud is detected preemptively, it is detected faster and results in lower losses; conversely, passive detection results in longer-lasting strategies and greater financial damage to the victim. Above mentioned anti-fraud controls such as account reconciliation, automated transaction/data monitoring, ongoing surveillance and proactive management review, and internal audit departments are all tools that can help detect occupational fraud more effectively. Automated data monitoring leads to the detection of fraud in around six months, meaning that the loss of the organization is lower (at around $50,000) when compared to passive detection methods, such as confessions, which can take 14 months and lead to a loss of almost $160,000 (ACFE, 2022, p. 23).

Red flags

Forensic accounting studies highlight the notion of "red flags" and how useful they are when discussing how fraud is detected. The authors Singleton & Singleton (2010) use the term red flags as a synonym for what they call the "fingerprints of fraud" (p. 95). In simple terms, they are indicators that can be used for a variety of purposes, including detecting potential fraud, and represent a meeting point between the prevention and detection systems, as they can both be used within a more structured anti-fraud risk management mechanism, to prevent the occurrence of illegal facts by lighting a "danger signal" in the areas most at risk, as well as detecting something that has already occurred and techniques that can be used by all actors in the internal control system, but also by external statutory auditors and forensic consultants because, due to their potential simplicity, they do not necessitate in-depth knowledge of the fraud. As the authors roughly explain, whenever fraud occurs, there always seem to be remnants of the crime left at a crime scene, and the same logic also works for fraud detection.

Notorious cases such as Enron and Worldcom are all examples of fraud that have

worsened due to auditor negligence, frauds that are included in the fraudulent financial reporting area of the study. As El-Aziz & Kassem (2010) explain in their work, in various cases, it can be stated that during the audits, the auditors failed to obtain relevant evidence or to recognize and follow up on red flags. Moreover, external auditors have a known history of counting on internal controls as the strong and primary defense for fraud prevention. However, as it has been widely demonstrated, this system can only sometimes work with the employees as they can override such controls, sometimes even with ease.

Examples of red flags include unjustified transactions or events, accounting anomalies, unusual elements within a transaction, changes in the behaviour of people or the characteristics of the business, or they can be thought of to identify characteristics usually associated with the most common fraud schemes. However, the presence of a single red flag does not produce an appreciable meaning; instead, an individual or employer must wait for a combination of more of them to request an in-depth investigation. Some red flags, as previously stated, can be used by those who are not specialized in fraud research and are primarily those that arise from the so-called risk factors, that is, the context in which the entity operates and - in other words - the fraud triangle (opportunities, motivations, and rationalization): these are the so-called behavioural red-flags, which find space in this introductory paragraph of detection methods.

The experts describe certain behavioural traits associated with fraudulent behaviour in the ACFE's 2022 Report to the Nation. The ACFE study usually lasts a year, which means that the fraudster could have been displaying warning signs that could aid in the early detection of fraud long before it was committed.

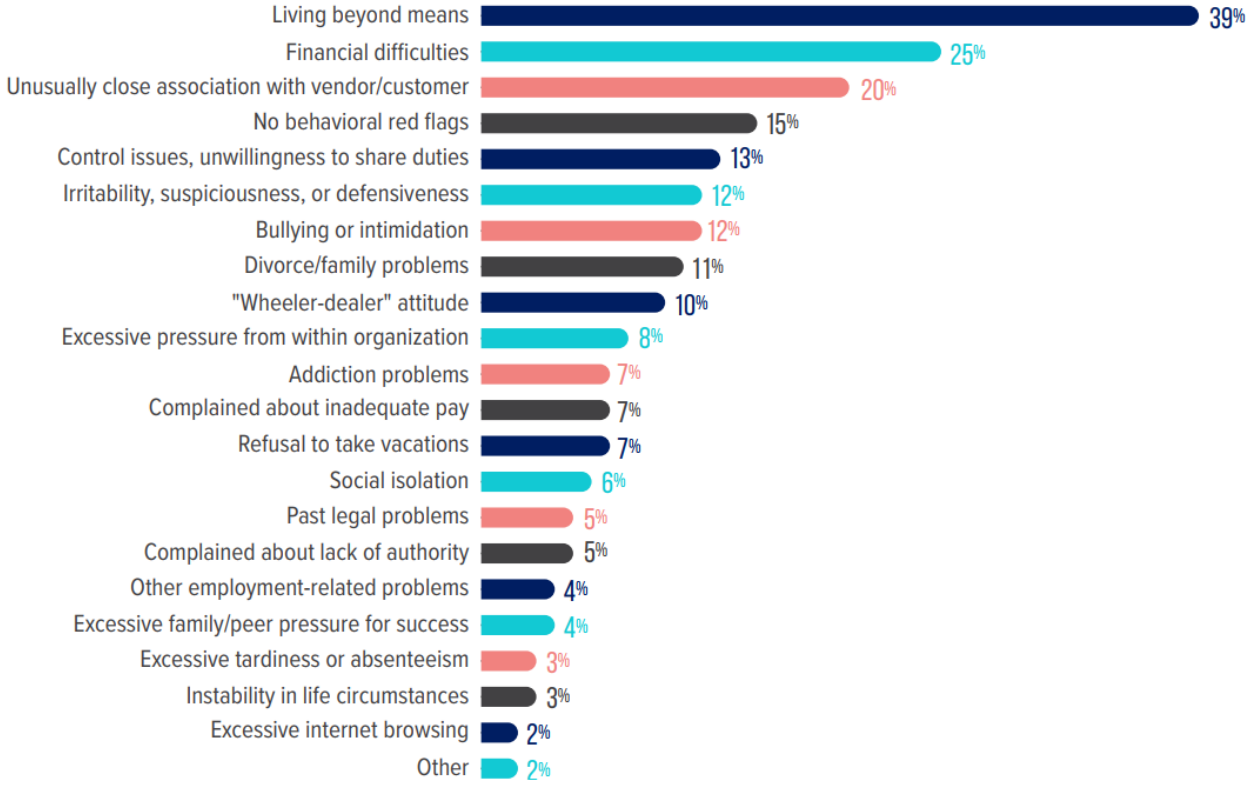


Fig. 13 - How often do perpetrators exhibit behavioral red flags? [13]

As shown in the picture, the study focused on presenting the surveyed respondents with a list of the most common behavioural red flags (20 total) and how these have been noticed in the perpetrator over time (Singleton & Singleton, 2010, p. 99). The study shows that in 85% of the fraud cases, there was at least one red flag identified and that in 51% of the cases, there was even more than one of the listed red flags. Accordingly, the most common red flags detected were living beyond means, financial difficulties for the perpetrator, unusually close relationships with customers or vendors, and unwillingness to share duties which leads to excessive control issues (ACFE, 2022, p. 59).

[13] Retrieved from page 58 (Ibid).

Red flags in different fraud schemes

The authors Singleton & Singleton, in their book "Fraud Auditing and Forensic Accounting" (2010), differentiate different categories of red flags based on different types of fraud. As explained in their dedicated chapter (pp. 99-111), the most common type of fraud (as already mentioned in this research) is financial statement fraud. The authors distinguish a list of red flags which are most commonly found in these illicit schemes: accounting anomalies, unusual profits, the rapid growth of the perpetrator, internal control weaknesses, the aggressiveness of the executive management, the micromanagement done by the latter, as well as the general obsession over stock prices. The most common of these concerns is the administration workstyle which, for example, may constantly think and approve overly optimistic financial goals (which would then provide the typical pressure at the base of the fraud triangle).

Regarding red flags most commonly found in asset misappropriation schemes, it is crucial to underline how the organization's employees usually perpetrate such frauds for their benefit. According to Lux & Fitiani (2002, pp. 50-51), the most common behavioural red flags include the perpetrator's: increased irritability, changes in behaviour, inability to look at others in the eyes, tendency to blame others, irregular work history, changes in the lifestyle, as well as the presence of consistent anger. In the case of asset misappropriation, the changes in the lifestyle of an employee are usually the brightest red flags that should be looked after as the perpetrator will always seek to become more successful and if the organization was incapable of noticing the loss of a specific amount (for instance 10,000 dollars) the employee will try to get away with an even higher amount the second time (for instance 20,000 dollars). Singleton & Singleton also add other red flags to this list, describing how great attention should be paid to employees who have financial problems, never take a vacation, reject

promotions, constantly complain about how the employer treats them, and even exhibit psychotic problems (p. 102).

Lastly, corruption schemes are usually perpetrated by employees as well, always for their benefit against the company. Generic behavioural red flags typically involve lifestyle changes. However, they can also include anomalies in approving vendors for a specific transaction, anomalies in the recording of said transactions, secrecy around third-party relationships, such relationships existing between them and the vendors who were authorized and chosen, as well as the lack of review on management approvals which are unaware of the existing relationships (Ibid, p. 108).

Chapter four

IV. Forensic Accounting techniques

"Fraud is here to stay. The only really surprising fact is that people are still surprised by the discovery of fraud. The financial press and the popular press regularly report on the largest cases. It seems that when people are given the opportunity to commit fraud, many do indeed commit fraud" (Nigrini, 2011, p. 452).

With the advancement of technology and the acquisition of more modern technical and technological aids, forensic accountants can assess the correctness of a company's operation more rationally and reliably. Work is completed faster, judgment is less risky, and results are more likely and accurate. Accounting solutions allow us to conduct more complex and extensive research and evaluation procedures without incurring additional costs or time. A forensic accountant is expected to be well-versed in the tools that aid him in the investigation, ensuring the credibility of the results obtained.

Accordingly, these tools require the forensic accountant to be familiar with digital forensic skills, which can be both basic and advanced. In the first case, the only capacities needed are acquiring and collecting data from computers and other electronic devices. In contrast, in the second case, there are other capacities required. This so-called digital forensic science has already been discussed. In 2001 at the first "Digital Forensic Research Workshop" that took place on the 7 and 8 of August 2001 in Utica (New York), the science of digital forensics was explained as using "scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (Johnson, 2014).

The Certified Forensic Computer Examiner (CFCE) was the initial Anglo-Saxon certification to demonstrate computer forensics skills in Windows-based computers (ISFCE). These skills include but are not limited to: knowing how to acquire data from a complex accounting system, how to examine, analyze, and report on it as well as the knowledge in collecting all of this data from the company's systems. These forensic accountants typically can execute a set of data queries directly on the target system, making simple extractions, extracting data with complex criteria selected, checking for any duplicates or missing data, and even identifying "holes" in the sequences. Following are some of the most used auditing tools that help in the field of fraud prevention although it needs to be underlined that forensic data analysis is only one part of the fraud investigation process; an entire investigation cannot be based solely on computer calculations and must include a review of paper documentation (including contracts and budgets), interviews, reports, linear reasoning, and solid conclusive considerations.

i. Computer Assisted Auditing Tools (CAATs)

Forensic analysis of financial data thus refers to examining a large number of financial transactions to detect signs of error or fraud. Combining different documents, accounts, and - in some cases - even different companies makes this much more effective. A forensic analyst must have specific technical knowledge, including accounting knowledge (those as mentioned above "common basis"), in-depth computer skills and the ability to create reports and considerations based on the analyses performed. For this reason, one of the useful tools is CAATs. So, what are CAATs? They are tools and techniques that enable auditors to significantly improve efficiency and effectiveness during the audit's planning, testing, and reporting phases. These tools

include operating systems such as business intelligence audit technology, database applications, and electronic auditing. CAATTs, sometimes also referred to as general purposes software (GAS), play important roles in reducing audit costs, improving audit productivity and quality (Bierstaker et al., 2014), and are constantly expanding their use in advanced societies (Lowe et al., 2017 and Siew & Yeow, 2020).

As Crain et al. (2015) explain in their book, GAS and CAATs' primary functions include data extraction from accounting and perhaps even ERP systems. CAATs also includes a plethora of tools for evaluating extracted data. In some cases, sophisticated CAATs may "plug in" to the target accounting system, allowing the forensic auditor to conduct complex queries directly from the targeted system. In contrast, the forensic auditor will "dump" the system's data into one or more files that the CAAT can process. Some of the functions of these tools include sophisticated data queries, sample extractions, completion checks, duplicate checks, reasonable checks, missing sequence identification, statistical analysis (such as Benford's law) and calculations as well as reasonableness checks. Furthermore, CAATTs can be used in several approaches to logic application, such as parallel simulation (the forensic auditor reprocesses transactions produced by the target system using a system separate from the target system.), integrated test facility (incorporating an audit module in the software code of the target system) and test data (test transactions are submitted to the target system by the forensic auditor) (Ibid, p. 323).

CAAT tools offer a set of predefined functions for performing quick data analysis. They also typically include functions that allow them to perform more complex analyses by performing operations on the input fields (without modifying them) (Al-Okaily et al., 2022, pp. 31-58). As a result, it is possible to classify income statements with fewer entries, identify users with fewer entries, check the length and content of certain fields,

perform operations on dates, apply filters to selections, and even relate different tables. Furthermore, these tools allow grouping a series of commands within a script to automate the most repetitive tasks. This method is especially useful for implementing a continuous auditing process at predetermined intervals (Curtis & Payne, 2014, pp. 304-308).

Forensic accountants can use CAATs as an efficient and effective tool to achieve their audit objectives (Axelsen et al., 2017, pp. 15-31). Some benefits of using them in fraud auditing and elsewhere include the examination of all the data instead of just a sample, the procedures and commands are usually already familiar to auditors (meaning that there will be a short learning curve), the advanced tools even allow for automatic documentation of the audit results and such results can be imported in various formats and, lastly, these tools use a copy of the necessary data, meaning that no modifications are allowed (read-only).

ii. Data Mining Techniques

When speaking of data mining, the subject regards a set of statistical techniques specifically designed to automatically mine large amounts of data for new, hidden, or unexpected information or patterns. According to the CGMA (2013), data mining is among the most critical and important frameworks of advanced intelligent business data analysis and decision support tools. The major professional accounting bodies recognize the importance of this, as it has been identified as one of the top ten technologies for tomorrow by the American Institute of Certified Public Accountants (AICPA). Data mining as one of the four research priorities of the Institute of Internal Auditors (IIA) (Han et al., 2006). Furthermore, according to Chartered Global Management

Accountants (CGMA), around 50% of business leaders believe that data mining and the use of big data are among the top ten priorities in the corporate world, critical for the data-driven era of business (CGMA, 2013).

There are many benefits that these techniques bring to the table, for instance, aiding senior managers in the decision-making process, raising the company's competitiveness as well an effective prediction of the organization's future development (Xiao & Gaojin, 2010, pp. 381-4). Data mining enables companies to more easily identify statistical relationships among performance measures and estimate the likelihood of an event occurring, thus supplementing managers' qualitative judgments and providing a control vehicle for data accuracy and legitimacy. Furthermore, these tools also help organizations rapidly decipher patterns in data that would take years to discover using older techniques, identify disgruntled employees based on patterns in their email exchanges, and provide the federal authority with real-time market surveillance and risk profiling of market participants (Agyemang et al., 2006, pp. 521-538).

There are three data mining techniques: discovery, predictive modelling, deviation and link analysis. It discovers common knowledge or patterns in data without any prior knowledge of fraud, hence, without any predefined idea or hypothesis about what the pattern might be. In the form of conditional logic, it exhibits various affinities, associations, trends, and variations. Patterns identified in the database are used in predictive models to forecast outcomes and guess data for new value items (Granlund et al., 2013, pp. 275-277). Whereas description is concerned with identifying human-interpretable patterns in the data, prediction is concerned with using some fields or variables in the database to forecast unidentified or prospective values of other important variables (Williams, 2013, pp. 544-558). Prescription, on the other hand, concentrates on providing the most effective solution for the given issue. Many data

mining tasks, such as classification, outlier detection, visualization, clustering, prediction, and regression, can be used to achieve these goals.

Classification is concerned with mapping data to a set of predefined qualitative separate attribute classes, which can be binary or multi-class and uses a model to predict the categorical tags of unknown objects to distinguish between items of various classes. These are predefined, discrete, and unordered categorical labels (Amani & Fadlalla, 2017, pp. 32-58). Outlier detection is concerned with locating data that deviates significantly from the norm. It uses detection distance measurements between data objects to identify objects that are distinguishable from or inconstant with the remaining data set. Outliers are data that appear to have distinct traits from the remainder of the population (Ahmed, 2004, pp. 455-459).

Furthermore, visualization is concerned with the presentation and comprehension of data. It ensures that data is presented understandably by employing a methodology that converts complex data characteristics into straightforward trends, allowing users to understand the complicated patterns or relationships discovered during the data mining process (Zhang & Zhou, 2004, pp. 513-522). Clustering is concerned with segmenting data into useful classes or groups, and it is also referred to as data fragmentation or partitioning since it is a type of unsupervised classification (Yue et al., 2007, pp. 5519-5522). Prediction deals with predicting a future numerical or non-numerical value based on the "patterns" of the data; lastly, regression is a statistical methodology used to reveal the connection between one or more independent variables and a continuous-valued dependent variable, and it is commonly used in the detection corporate fraud, automobile insurance, and credit card fraud (Yamanishi et al., 2004, p. 276). The norm is found first in deviation analysis, and then items that deviate from the norm within a given threshold are detected (to find anomalies by extracted patterns). Recently, link

discovery has emerged as a method for detecting a suspicious pattern by primarily employing deterministic graphical techniques and Bayesian probabilistic casual networks. The "pattern matching" algorithm is used in this method to 'extract' any unusual or suspicious cases (Turba et al., 2007).

iii. Ratio Analysis

Ratio analysis measures the relationships between different financial statement items as well as these items and nonfinancial data. It is a forensic accounting technique used to compare on a historical, industry, or against a defined benchmark basis. It detects fraud by examining data patterns to identify potentially fraudulent transactions. There are various ratios, such as liquidity ratios, profitability ratios, solvency ratios, coverage and efficiency ratios, and market prospect ratios. A financial expert uses ratio analysis to determine the relationships between specific costs and production measures such as units sold, dollars of sales, or direct labour hours. For example, overhead costs per direct labour hour can be calculated by dividing total overhead costs by total direct labour hours and can assist in estimating expenses (Mousa, 2016, pp. 553-570).

iv. Benford's Law

Forensic data analysis project is an iterative procedure: once a potential inconsistency is discovered, it is necessary to dig deeper and investigate that behavior and transaction to confirm the anomaly and, if present, the underlying causes.

Benford's law is one that can be used in forensic accounting to determine whether our data is reliable or fictitious. This law can serve as a starting point for further

investigations for the forensic accountant if the calculation reveals that the first numbers are distributed differently than they should be. The law is based on an unusual observation of digits, namely that some digits appear more frequently in data sets than others. It has been determined that the digit 1 appears the most frequently at the beginning of the numbers and that each subsequent 2, 3, up to 9 is a certain percentage less than the previous one. The table shows the percentages of repetitions of the first digit from 1 to 9 (Durtschi et al., 2004).

During the investigation of fraudulent acts, the following facts were established using Benford's law (Nigrini, 1999): scams begin with small sums and progress to larger sums and when increasing sums, the threshold sums beginning with 1 are usually not exceeded (for instance 1,000, 10,000, 100,000). Threshold sums represent a psychological limit and, in many cases, a limit for the competent person's approval of higher sums. Lastly, to avoid additional approval or control, the numbers 7, 8, and 9 are frequently used for the most extracted sum, which is the inverse of Benford's law. Scams can only be detected in this manner if the frequency of the distribution of first-digit combinations is present. Its main benefit is detecting unusually composed numbers or amounts in the selected data set. In forensics, it serves as an investigation when we want to check the accuracy of accounting data, the company's market value, receivables, prices, stocks, duplicate payments, the implementation of a new computer system, sales price calculations, customer compensation, and supplier obligations. However, we cannot use it for all numbers of a specific pattern, such as different bank account numbers, identification numbers, health insurance numbers and others (Nigrini, 2022).

Benford's law adds another layer to the investigative process to detect fraud. Many real-world data sets have provided evidence for this law (river surfaces, populations). Because this rule is not intuitive, those who "invent" the numbers frequently produce a

pseudo-random that does not correspond to the real cases. So, if the distribution of frequencies reveals one which does not comply and, therefore, where first digits differ significantly from Benford's law, it could be due to data deception and, hence, there is a risk of fraud (Crain et al., 2015, p. 222).

v. Theory of Relative Size Factors (RSF)

The theory of relative size factor (hereinafter referred to as RSF) can detect outliers or unusual data that could be caused by errors or fraud, and it quantifies the ratio of the biggest to second biggest number in a given data set, so records that do not fall within the prescribed range are suspected of being errors that need to be investigated further. The boundary lines that each region has define the area. A transaction is considered suspicious if it fails to meet specific requirements (Crumbley, 2001, pp. 181-202). This theory reveals a data set or elements that are considered outliers that are not considered commonplace. The main principle of this method is based on the understanding that transactions should have a distribution that is considered normal, while other distributions cannot be considered normal. This relative size factor theory reveals a data set or elements that are considered outliers that are not considered commonplace. The principle of this method is based on the understanding that transactions should have a distribution that is considered normal, while other distributions cannot be considered normal (Panigrahi, 2006, pp. 1426-1430).

$$\text{Relative Size Factor} = \frac{\text{Largest Record in a Subset}}{\text{Second Largest Record in a Subset}} \quad [14]$$

[14] Formula of relative size factor theory from page 213 in
Nigrini, Mark J. (2011). *"Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations".* 1. Vol. 1. Hoboken, New Jersey: John Wiley & Sons Inc.

The relative size technique of analysis is a practical error detection tool. The test examines subsets in which the most significant amount differs from the others in that subset. This difference could be due to the most extensive record either belonging to another subset or belonging to the subset in question but having the numeric amount incorrectly recorded.

This investigative analytics test typically runs with the largest and second-largest numbers in each subset. Depending on what is considered an outlier, forensic investigators can modify this formula to draw attention to it. Adjustments include the greatest amount divided by the median amount, the biggest divided by the average, the average excluding the most significant number, and the smallest number divided by the average, which is usually utilized to look for understatements (Nigrini, 2011, p. 213).

Chapter five

V. Internal Controls

As already explained in a previous chapter, fraud is made up of three components: perceived pressure, perceived opportunity, and rationalization of the fraudulent act (Albrecht, 2009), and since all frauds share these three characteristics, it is crucial to understand where the weaknesses in an organization are. Inevitably, the absence of proactive fraud audit procedures to prevent fraud is cited as a major contributor to the emergence of fraud. Even if there is no deception threat, the audit, which can be done in conjunction with a person's or company's significant knowledge and ability to handle current funds, can quickly reveal. Moreover, the efficiency of internal controls leads to the prevention of potential fraud and reporting false accounting reports. Various methods, guidelines, and projects are used to protect funds better, prevent fraud, and ensure that financial data is precise and authentic. Internal control must be performed correctly to avoid fraud (Chen et al., 2018 and Barzinji, 2022).

So what is meant by the term internal control? Financial policies, accounting procedures, internal processes, authorization and approval systems, checks and balances, and duties segregation are all internal controls. Nevertheless, internal controls are much more than that, beginning with the organization's overall climate or the "tone at the top" culture (Pedneault & Rudewicz, 2012, pp. 98-101). As a result, it is a continuous activity carried out by all corporate bodies, permeating all business units and becoming an integral part of daily activity. According to the 2012 PwC study on "Internal Audit," internal controls are a company's methods for ensuring the integrity of financial and accounting information, meeting operational and profitability targets, and disseminating management policies throughout the organization. Every internal control

must have three components in order to be effective: expectations, compliance, and consequences, and the controls will be ineffective if one of them is missing. A carefully designed internal control system will begin with the role of the board of directors in the organization and continue down to the most basic functions and responsibilities. Internal auditors conduct audits in larger organizations to ensure compliance with controls and procedures and identify occurrences of possible fraud or abuse, thereby strengthening internal controls (Pedneault & Rudewicz, 2012).

The International Standards of Auditing (ISA 400) define internal control as all policies and procedures adopted by an entity's management to assist in achieving management's goal of assuring, as far as possible, the orderly conduct of its business, including asset safeguarding, adherence to management policies, the prevention and fraud detection and error, the accuracy and completeness of accounting records, and the timely preparation of financial statements (ISAAB).

The Security and Exchange Commission (SEC) does not officially require internal controls but articulates broad goals controls should achieve, where issuers are responsible for implementing specific policies and procedures. Several factors are usually considered in determining whether an internal control system is reasonable under the circumstances. The factors include the role of the board of directors, the corporate procedure communication, the personnel competency and integrity, the delegation of authority and responsibility, the accountability for performance and compliance with policies and procedures, and lastly, the impartiality and effectiveness of internal audit function (Crain et al., 2015, p. 523)

On the other hand, the Foreign Corrupt Practices Act of 1934 (FCPA) enforces recordkeeping and internal control requirements and prohibits the payment of corrupt payments. The recordkeeping requirements require adequate detailed recordkeeping.

Internal control requirements include the provision or requirement of a system of internal controls to provide or require: reasonable assurances that transactions are carried out per management's authorization, asset recording and accountability required to generate correct financial statements, and access to assets are restricted by management's authorization. Furthermore, the FCPA requires publicly traded companies to design and maintain an internal control system adequate to provide reasonable assurances that transactions are performed under management's general or specific authorization and that records of the transactions are kept as necessary to permit the prepping of financial statements following GAAP or any other criteria relevant to such statements and to ensure accountability for assets and that access to assets is restricted (Ibid). Implementing this management tool allows the company to ensure a certain level of efficiency in the performance of its operations, good use of its resources, and compliance. This management tool adds value to the company because it knows how to adapt the system to its structure, environment, and changes. It is part of a continuous improvement process and must first target effectiveness (achieving objectives) and efficiency (cost/profit).

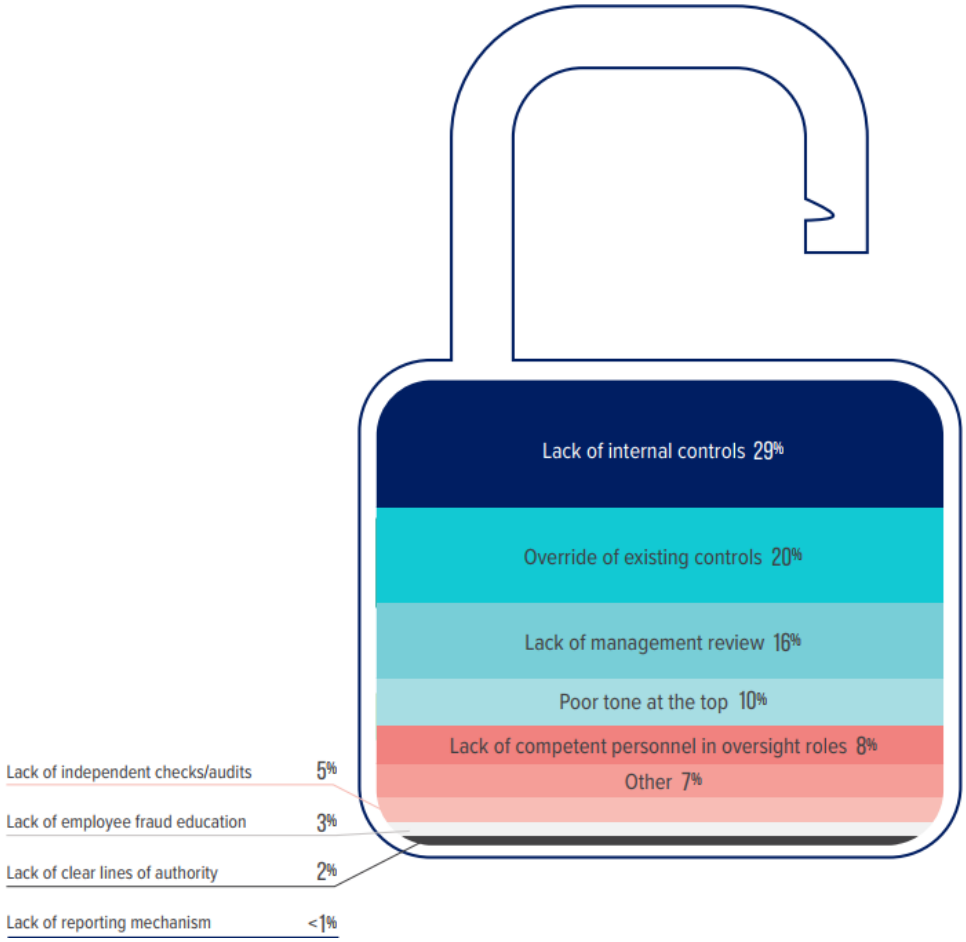


Fig.12 - What are the primary internal control weaknesses that contribute to occupational fraud? [15]

[15] Scheme retrieved from page 42 (Ibid).

Organizations with functioning anti-fraud programs still have to deal with the emergence of fraud yearly. In ACFE's (2022) Report to the Nations, there was a study on the main internal control weaknesses that led to fraud. As shown in the figure, in 29% of the cases, the main reason why fraud occurred was due to a lack of internal controls, meaning that most victim organizations lacked appropriate controls to prevent fraud. Furthermore, in 20% of the cases, there was an "override" of the internal controls, meaning that the perpetrator had easily circumvented the mechanisms that the organization for fraud prevention had implemented. Overall, this graph demonstrates that most of the frauds that occur yearly could have been prevented with the use and implementation of an improved anti-fraud control system (p. 42).

i. Internal control frameworks

COSO

Internal control is used to ensure compliance with laws and regulations, as well as compliance with the hierarchy's instructions for the company's strategy. It also ensures the smooth operation of the company's processes, as well as some transparency and dependability in financial information communication.

The early 1980s savings and loans scandals resulted in the formation of the National Commission on Fraudulent Financial Reporting (popularly called the Treadway Commission, named after the Commission's chair), which continued its tasks as the Committee of Sponsoring Organizations (COSO), which is still in operation today. This committee is a non-profit commission that has developed a framework for establishing an internal control system (or for evaluating and updating the procedures in place). This

standard defines the guidelines through five components and 17 principles that establish an internally effective control system within an organization. According to the findings of the Treadway Commission, the most efficient way to preclude financial scandals, such as the savings and loan scandal, is for businesses to have a powerful set of internal controls. The Commission's publication aimed specifically at improving the quality of company financial reports by focusing more on corporate management, ethical standards, and internal control. The group's model has been referred to as the COSO Model of Internal Controls (Singleton & Singleton, 2010, pp. 10-1).

This Model of Internal Controls focuses on five main areas, namely risk assessment, control environment, information and communication, monitoring and control activities. Regarding risk assessment, this task requires the identification and analysis of risks relevant to the entity's objectives as a foundation for defining how all those risks are managed and controlled. Though since economic, regulatory, industry, and operating conditions are constantly changing, mechanisms for identifying and dealing with risks are required on an ongoing basis. The control environment is the foundation for all components of internal control, supplying structure and discipline and influencing organizational personnel's control awareness. Such control environment factors include the organization's people's integrity, ethical values, and competence; management's philosophy and operating style; management's approach to assigning responsibility and authority and how staff members are organized and developed. Following, a successful organization undoubtedly necessitates on working information systems that generate reports with financial, operational, and compliance data required for informed decision-making. Moreover, communication should also flow down, up, and throughout the organization so that employees understand their roles and how they correspond to others. Furthermore, communication skills are required with external parties such as

suppliers, customers, regulators, investors, and other stakeholders. Monitoring is crucial as o system can be simultaneously successful and static at the same time. It should be tracked and assessed for changes and improvements brought about by changing circumstances and the scope and frequency of internal control structure evaluations are determined by risk assessments and the greater perceived internal control system and its effectiveness annually. Lastly, control activities are those that take place all over an organization, and their main role is to assist management directives as well as the implementation of policies and procedures. Furthermore, these activities help to ensure that the necessary steps are taken to manage the risks which may prevent the organization from meeting its objectives. Approvals, permissions, validations, reconciliations, operating performance reviews, security procedures over facilities and personnel, and segregation of duties are all examples of control activities (Skalak et al., 2011, pp. 20-1).

Fig. 13 – COSO cube for internal control[16]

[16] Image retrieved from Thabit, Thabit. (2019). *"Determining the Effectiveness of Internal Controls in Enterprise Risk Management Based on COSO Recommendations."* SSRN. nternational Conference on Accounting, Business Economics and Politics. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3401199.

It can be said that the past decade has highlighted some of the major challenges companies have faced in trying to implement framework, such as integration of strategy definition processes, and involvement of such framework. Furthermore, there has been an uprising in the diffusion of enterprise risk management systems (ERM), especially following the 2008 financial crisis, the advancements and dependence on technology, meaning that organizations today are forced to face continuously evolving crises that they never faced before. The complexity of these new company contexts as well as the general volatility of the business sector has brough a new light in the essentialism of risk assessment. Inevitably, all these changes led to the ever-growing necessity of an update of the COSO framework.

The original repository, established in 1992, has undergone some changes due to new regulations (Sarbanes-Oxley, financial security law) enacted in the aftermath of various financial and accounting scandals such as WorldCom and Enron. There have been several developments between the first COSO (Internal Control-Integrated Framework, 1992) and its updates, including the addition of seventeen principles that take into account technological advances and fraud in risk assessment. The is no longer only concerned with financial reporting but also operational and compliance goals. On the other hand, it is also concerned with CSR (societal and environmental responsibility) and safety and has prominently articulated the concept of "tone at the top." Another innovation COSO (2013) introduced is the establishment of "lines of defense" within the organization, which is critical in the fight against fraud. Indeed, several internal control actors stand out within a company, each with a specific role to respect (ANRA, 2020).

Fig. 14 – COSO cube for ERM [17]

Nevertheless, there was another update in 2017 with a framework based on the premise that every organization exists to create value for its stakeholders and manage the uncertainties in increasing this value. There is an updated definition to the term uncertainty which now signifies "something unknown" while the term risk is described as the effect that said uncertainty has on both the formulation and the execution of a business strategy leading up to the achievement of company goals.

The new endeavor now is to understand how much of both the company can handle, meaning that the ERM framework has to assure that there is an overall optimization between risk exposure and opportunity that can lead to the strengthening of the company's ability to generate and preserve value.

[17] Image retrieved – (Ibid)

This new framework focuses on the role of ERM in defining and executing corporate strategy, it strengthens the alignment between ERM and corporate performance, it follows up on expectations in terms of governance and supervision, it presents new ways of interpreting risk in a complex business context, and it also underlines the role of risk reporting in responding to stakeholders' expectations of greater transparency while also incorporaing new technologies and greater use of data analytics to support decision-making (Dias, 2017).

Furthermore, the updated COSO framework introduces five interconnected components: risk governance and culture, risk in execution, risk strategy and objective setting, risk information communication, reporting, and monitoring risk management performance (Ibid, p. 79). Regarding the first component, there would not be a solid and efficient ERM system without risk governance and culture. Some of the principles include encouraging the implementation of the board's risk management guidelines, sharing ethical values and integrity by the entire organization, and strengthening accountability on risk matters at all levels of the organization.

Risk in execution refers to the risks that can affect the implementation of the strategy and business objectives and must be identified, assessed, and addressed through specific response actions that take risk into account. Some principles include assessing each risk's severity using qualitative or quantitative approaches, prioritizing risks based on metrics relevant to the organization and defined risk tolerances, and developing a portfolio view of the risks that can influence business objectives.

Although many organizations focus primarily on risks during strategy execution, it is necessary to anticipate the focus of the ERM during strategy definition in order to understand how the corporate risk profile may change as a result of decisions made.

In this case, some of the principles include analyzing risk and the internal and external business context that generates it, defining risk appetite in line with the company's vision and fundamental values and communicating it to the entire organization, and evaluating alternative strategies / different strategic options while taking their corporate risk profile into account. Risk information, communication, and reporting emphasize the importance of a continuous process of gathering and sharing relevant internal and external information that allows the organization to make informed decisions. The final component focuses on monitoring the risk management model's results and the effectiveness of the framework's individual components over time. Effective monitoring processes help the organization recognize the connection between risk and corporate performance. Monitoring significant changes in the context, which can compromise company performance and nullify the assumptions underlying the strategies adopted, is one of the reference principles, as is monitoring the ERM process with a view to constant improvement to increase its added value systematically (Thabit, 2019).

Recognizing the impossibility of proposing a "universal" solution that applies to all organizations, the new COSO Framework suggests a set of general principles. Each organization must consider its particularities in terms of strategy, organizational model, culture, operating model, available financial instruments, sector to which it belongs, and so on to effectively implement the framework.

Sarbanes-Oxley Act

Sarbanes-Oxley was and continues to be an attempt to help prevent such accounting scandals as those at Enron, WorldCom, Adelphia, Peregrine Systems, and Tyco International. These scandals harmed investor sentiment in United States businesses and cost shareholders billions of dollars when stock prices fell and the country's security markets were severely shaken. Since the United States approved the Sarbanes-Oxley Act in 2012, which imposed new obligations on businesses due to corporate fraud prevention becoming an important issue.

The legislation aimed to restore public trust after major corporate scandals like Enron had eroded it. Companies must have an internal audit system under Section 404 of the Sarbanes-Oxley Act. The goal is to increase investor confidence by ensuring systematic preventive action against corporate fraud. As internal audit functions have emerged, fraud prevention methodologies have become increasingly crucial in companies outside the United States.

Signed on July 30, 2002, the official goal of this act was to "protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes" (United States Congress, 2002). The act's regulations are divided into eleven chapters or titles, each addressing a particular issue. The first one established the Public Company Accounting Oversight Board (PCAOB), as mentioned earlier, which is a non-profit organization that controls auditors for publicly traded companies whose mission is to reduce audit risk. To do so, it enforces adherence to the Sarbanes-Oxley Act and establishes auditing standards. The second section deals with the crucial element of the auditor independence standard by including a section on conflicts of interest and a mandatory rotation of audit partners.

The third title deals with Corporate Responsibility and explains that audit

committees are required for public companies and how corporations are also held accountable for specific actions related to financial reports. Any failure to comply will result in fines and penalties for executives. Title four regards enhanced financial disclosures, meaning that additional disclosures provide a more accurate picture of a company's financial statements than just financial reports. Title five (analyst conflicts of interest) boosts investor confidence in securities analysts' reporting. The sixth outlines various practices, such as the SEC's jurisdiction to remove somebody from their position as a broker, advisor, or dealer if certain conditions are met. Title seven regards how the SEC is required to conduct studies and reports, while eight deals with corporate and criminal fraud accountability. Nine aims to strengthen criminal sanctions for white-collar crime, while ten requires the Chief Executive Officer to sign company tax returns. Lastly, title eleven, the most interesting for forensic accountants, comprises seven sections devoted to corporate fraud as it makes tampering with records a criminal offense punishable by specific penalties while establishing guidelines for sentencing and increasing overall penalties (Sarbanes-Oxley, 2002).

According to Brickey (2003), not long after the implementation of this act, there was an increase in penalties that provided an important incentive for individuals involved in significant corporate investigations to join into the contractual arrangements with the government. Accordingly, the maximum terms and financial penalties for securities fraud have been doubled, and penalties for mail and wire fraud have indeed been quadrupled. Because the largest category of fraud is the one this study focused on, occupational fraud, it is crucial to understand whether this legislation has brought changes in this specific fraudulent acts. Following a research study by Alleyne & Elson in 2013, the overall general occupational fraud occurrences increased following the implementation of this act, while the median dollar loss decreased dramatically. In other

fraud schemes, such as cash larceny, the occurrence of such schemes had a downward trend and the percentage of other fraudulent disbursement incidents decreased steadily.

Nevertheless, a different study conducted in 2015 (Gray et al.) decided to investigate thirty various accounting fraud cases discovered between 2010 and 2013 in multiple industries. The aim was to compare the effectiveness of Sarbanes-Oxley and the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act. The result of the study was that SOX alone was insufficient to improve the financial stability of the United States.

The cases of fraud that took place ten years after the implementation of this act (in 2012) also included famous scandals such as Bank of America, Adobe, and Groupon, where the main focus was on weak internal controls and data breaches. Following these cases in 2013, there were more scandals (Bitcoin and Walmart) which brought to the attention the fact that the existing regulation is insufficient to dissuade the increasing amount of cyber-fraud activities caused by the increase in technological sophistication (this issue may be better suited for forensic accountants and auditors to develop expertise in detecting and preventing such fraud cases). Overall, Gray et al. implied in their study that Sarbanes-Oxley may have improved the fraud detection process, so the number of cases reported creates the illusion that more fraud activity is taking place.

Nevertheless, as had already been highlighted in a 2012 study (Udeh), The likelihood of auditor litigation has increased following Sarbanes Oxley, while the probability of litigation decreases for firms that are accelerated filers of the act. As of 2022, the Sarbanes-Oxley Act states all financial reports to include an Internal Controls Report, which shows how a company's financial data is accurate and adequate controls are in place to protect financial data. Another change was adding a year-end financial disclosure report, which requires a SOX auditor to review policies, procedures, and

controls during a Section 404 audit.

Furthermore, Section 806 of the Act authorizes the United States Department of Labor to protect whistleblower complaints against employers who retaliate and the Department of Justice to charge those responsible for the retaliation criminally (SOXCPA, 2022). The continuous updates are necessary to assure that the implementation of internal controls is followed, and the role of the forensic accountant is crucial in all of these practices.

Chapter six

VI. Advances in cybersecurity

On the other hand, cybercrime is a type of fraud that has recently gained traction and must thus be discussed in 2022. According to independent research conducted at McAfee's request in 2018, cybercrime is no longer just about lone hackers attacking personal computers from their bedrooms, driven by a spirit of challenge and personal achievement, but of an organized cyber mafia that mobilizes thousands of invisible computer networks to commit its misdeeds on a global scale.

Indeed, modern crime has adapted quickly to this new digitized world and has evolved substantially in response to technological advancements. These hackers can innovate in their attacks and exploit flaws in new systems poorly controlled and thus poorly protected by companies because of the new categories of devices, virtual networks, and computer architectures. According to a PricewaterhouseCoopers (2016) study, cyber fraud more than doubled in 2015. When it comes to stealing confidential data, this new virtual threat has the potential to be extremely powerful and effective. Hackers, in particular, employ the botnet, which is defined as a robot network connecting several thousand machines used in cyberattacks to hold companies hostage. As a result, cybercrime includes data theft, such as bank account access codes, and other types of confidential data stored in company computer systems, such as phone conversations, emails, or manufacturing secrets.

According to a study conducted by Ernst & Young in 2021, (Burg et al., 2021), current fiscal models are simply insufficient for what is essentially an existential threat. It is also indicative of many businesses' lack of understanding of cyber issues and inability to establish a security-by-design culture. Matter of fact, the survey respondents,

on average, had revenues of approximately $11 billion in 2020 while spending only $5.28 million, or 0.05% of the total, on cybersecurity per year, according to qualitative interviews with heads of cybersecurity and separately, as well as 1,010 senior cybersecurity professionals. To put it another way, very few businesses describe their safety funds as a varying and provisional expense of doing business. In practice, Chief Information Security Officers (CISOs) may struggle to scale the efforts of their functions in the context of specific and rapidly evolving business initiatives.

Nevertheless, forensic accounting and cybersecurity have joined forces to help define modern cybersecurity and bring black hat hackers to justice. Even though forensic accountants are not immediately responsible for security, they offer an essential service to investigators who are trying to piece together the complex steps that lead to a data breach. They may be asked to confirm that the data in breached systems has not been corrupted. How does this collaboration function? Forensic accountants can assist cybersecurity professionals in determining losses and justifying or disputing them in court by trying to investigate historical numbers and connecting them, such as via going through old financial statements, conducting interviews clients and employees, and reviewing budgets and economic forecasting data. Nevertheless, cybersecurity professionals are called in to assist forensic accountants with big data analysis, which is critical in analyzing this data (Wilson, 2022).

Essentially, it is the forensic accountant's responsibility to demonstrate that the numbers are correct. As a result, most major accounting firms now incorporate dedicated cybersecurity teams to acknowledge the significance of this specialty area. Their position is to acknowledge the implications of the technology used to manage accounting information systems. This demonstrates that, as discussed in the previous chapter, forensic accountants require a unique set of skills. To understand the stored

information, data system designers and users must comprehend the underlying principles of database and network systems. Although not all forensic accountants require formal coding training, programming is a required skill. As forensic accountants frequently interview subjects during investigations, they must be skilled at getting answers to their questions. Following the interviews, there is the crucial task of writing reports and documentation, which non-accountants will review, so clarity and precision are essential. Finally, creativity is required because the most extraordinary forensic accountants, like all other types of researchers, must be able to think outside the box to crack cases (Ibid).

The forensic accountant needs to take the appropriate steps, accordingly, prevention, loss mitigation and examination. In the prevention step, the forensic accountant must organize, prepare, detect, analyze, eradicate and recover the systems of an organization, as well as learn the processes and the evolution of the fraud in order to better the prevention capabilities of said organization. As more of our world becomes digital and more information becomes available at our fingertips, the expense of a cybersecurity breach must be considered, as a company's potential losses and damages can be devastating. A forensic accountant can assist organizations in determining what has been lost and quantifying the economic damages affiliated with a cybersecurity breach. Taking precautions to plan and minimize threats before an event occurs can be highly beneficial in the long run (Eide Bailly, 2020).

Chapter seven

VIII. Forensic accounting in Italy

Regarding fraud detection techniques in Italy, "traditional" reviewers must maintain professional skepticism and adhere to the procedures entrusted to them to seek the emergence and correct answers in the event of actual detection. The ISA 240 specifies the procedures for them. Nonetheless, there do not appear to be any ready-made textbooks or techniques for forensic accounting investigators (I had many difficulties finding information in Italian).

The main reason why there are extreme differences between the Anglo-Saxon internal control systems and the Italian ones are due to the diverse capitalism impositions that “Latin” countries have. Forensic accounting rose from the United States which, as explained in the previous chapters, has formulated acts and practices ad-hoc for this extremely crucial anti-fraud role. For instance, the Foreign Corrupt Practices Act (FCPA) that was already discussed in this study is represented in Italy by the D.gls 231/2001[18]. For the first time in our legal system, this legislative decree established a personal and direct responsibility of the collective entity (meaning both entities with legal personality and companies and associations even without legal personality) for the commission of a series of crimes by natural persons connected to it who acted in the entity's interest or to its advantage. This decree establishes the employee's and company's responsibilities in the event of offenses committed by its employees. In such cases, the employer can shield himself from legal action if he can show that he adopted and effectively implemented an organization, management, and control model appropriate for preventing crimes of the type that occurred.

[18] D.gls. 231/2001 - https://www.parlamento.it/parlam/leggi/deleghe/01231dl.htm

In addition to Legislative Decree 231, the following Italian national legislation and rules of reference that must be mentioned include: Legislative Decree 58 of 1998 ("TUF")[19] introduces the term "Internal Control System" (Article 149, paragraph 1, point c, "Duties of the Board of Statutory Auditors"). This decree assigns the task of supervising the adequacy of the organizational structure of the company for the aspects of its competence, the internal control system, and the administrative-accounting system, as well as the reliability of the latter in representing the management facts to the board of statutory auditors of listed companies.

Furthermore, there is the Corporate Governance Code for Listed Companies (Preda Code)[20], developed by the Borsa Italiana Corporate Governance Committee in 1999, and subsequent updates. The Preda Code defines internal control based on international frameworks; responsibilities for the internal control system are divided between the so-called and delegated bodies (concrete configuration of the system versus that of periodic verification).

Moreover, Legislative Decree No. 262 of 2005[21], entitled "Protection of Savings." It requires listed companies to appoint a new manager in charge of preparing corporate accounting documents (Article 154-bis of the TUF), who is responsible for developing adequate administrative and accounting procedures for the preparation of annual and consolidated financial statements, as well as certifying their adequacy and practical application in collaboration with the chief executive officer by imposing a specific supervisory obligation on the "effective compliance" of the board of directors procedures and intervening in the composition of the board of directors and the board of

[19] L.58/1998 - https://www.parlamento.it/parlam/leggi/deleghe/98058dl.htm

[20] Preda code - https://www.borsaitaliana.it/borsa/glossario/codice-preda.html

[21] D.gls. 262/2005 - https://www.parlamento.it/parlam/leggi/05262l.htm

statutory auditors to ensure the presence of minority representatives and the powers of the statutory auditors.

The Italian systems' corporate governance is made of the board of directors, the board of statutory auditors, the internal control and audit committee as well as the so-called supervisory body. If the articles of association or the shareholders' meeting allow it, the board of directors may appoint an executive committee or one or more managing directors. The board of directors establishes the scope, limits, and modalities for delegation. Said administrators deliberate on the company's management, call the assembly and set the agenda, take care of and keep the accounting records, create the financial statements that will be presented to the assembly for approval, execute the will of the shareholders' meeting and represent the company in third-party and legal proceedings (Pogliani et al., 2012).

The Board of Statutory Auditors serves as the control body for listed companies, supervising the activities of the directors and ensuring that the company's management and administration are carried out following the law and the articles of association. The duties of the board of statutory auditors are detailed in Article 149 of the TUF Law, which oversees compliance with the law and the articles of association, compliance with the principles of correct administration, and the adequacy of the company's organizational structure for the aspects of its competence. Furthermore, it supervises the internal control system and the administrative-accounting system, as well as the latter's dependability in correctly representing management events. It also overlooks the methods of the concrete implementation of corporate governance rules contemplated by codes of conduct drawn up by management companies of regulated markets or by trade associations, which the company declares to abide by, informing the public.

The Internal control and audit committee are responsible for overseeing the financial reporting process, the effectiveness of the internal control and internal audit systems, if applicable, risk management, the statutory audit of the annual accounts and consolidated accounts, and the independence of the statutory auditor or statutory auditing company, particularly concerning the provision of non-auditing services to the entity subject to the statutory audit. Finally, the supervisory body is responsible for constantly monitoring the observance of the Organizational Model issued by the body, its effective effectiveness in preventing crimes, the implementation of the provisions contained therein, and its updating if the Model needs to be adapted due to changes in the corporate structure and organization or the reference regulatory framework (Ibid).

It could be said that today, more than ever, specialization in the professional field has become essential due to the complexity and degree of analysis that has been achieved in every field; just as sophisticated are the mechanisms used to deploy scams and frauds of any kind, it is necessary to think of an Italian system that is capable of dealing with all of this. Although some efforts in this area are visible, the writer believes that the affirmation of alternative categories to the combination of chartered accountants and statutory auditors is still a long way off - as the opening lines emphasize. In Italy, professionals in the accounting field are currently classified as chartered accountants, auditors, and simple accountants, showing an apparent lack of forensic accountants even though the ACFE offers their certifications also in the nation and the leading auditing firms present (PwC, EY, and others) all deal with forensic accounting in the private sector.

Conclusion

This work's aim is to bring a focus on both the importance of forensic accounting today as well as depict the evolution that it has gone through while also suggesting some improvements. In today's world, enterprises are expanding to meet people's needs and provide the opportunity to provide services on a global scale as technologies for information and communication advance, increasing commercial activity volume. However, the benefits of such increases and developments are not without their drawbacks. That businesses do not. Examples of these negatives include failing to reflect the accurate results of their activities, changing numbers of their actual operating results, and rising the financial consequences of fraud and corruption. These factors have increased the demand for the forensic accounting profession to handle transactions that cause specialized research and expertise.

Forensic accountants are highly trained, experienced professionals with the accounting and legal knowledge required to resolve economic and commercial disputes. Forensic accountants are contacted in financial matters when judges decide because of a lack of information or disagreements. The mission undertaken by the profession's members to achieve unbiased views with their scepticism and researcher personalities is critical for these purposes. Thousands of frauds can hide behind regular figures, necessitating fully-equipped experts to uncover these frauds, as well as the insufficient financial understanding of judicial authorities in the decision-making process.

Forensic accountants are incredibly trained and skilled at detecting fraud in various ways. Their knowledge of accounting, law, criminology, and fraud equips them to detect and stop fraud schemes. Education choices are currently limited, though some schools offer degree courses in forensic accounting. However, solid knowledge of

financial auditing, its techniques and procedures, as a foundation, as well as creativity and ingenuity to design innovative procedures and techniques, depending on the case under investigation, are required. Often these forensic accountants start in tax or auditing and then move on to forensic accounting. Most forensic accountants also have a license that qualifies them for the job. It is critical to keep improving these educational and training opportunities to ensure that prospective forensic accountants are sufficiently prepared to carry out their duties.

The most crucial difference is that the forensic accountant, unlike the financial auditor, must have investigative and analytical capabilities and critical and strategic thinking to uncover simple and complex fraud schemes and their perpetrators and accomplices through almost imperceptible clues. Forensic accounting and professionals dedicated to its prevention, detection, and research have advanced the techniques for its discovery over the last two decades. They are now highly respected fraud fighters worldwide. Although they should have the necessary credentials and titles that demonstrate their specialized education, such as certifications provided by the Association of Certified Fraud Examiners, it is not required (ACFE).

Fraud, as an illness in our society, acts in such a way that it is not discovered until the consequences are almost irreversible, affecting not only those who work for the organization that is the victim of simple or elaborate fraud schemes but entire nations worldwide. Following several scandals involving corporate fraud, regulations, and despite regulations aimed at reducing or eliminating its occurrence and making detection and investigation easier, frauds continue to occur. Today, primarily through the internet, the business world's broadest spectrum tool. There are clear indicators of fraud, which many people ignore due to a lack of knowledge about them. It is through a deep understanding of the usual indicators and those created in the current to evade

controls or take advantage of a weak internal control system that allows the forensic audit professional to inquire about the fraud scheme.

In this study there is an extensive explanation and focus on fraud, especially occupational fraud, as it is the key reason as to why there is a necessity of all these internal and external controls in the first place. The Report to the Nations of 2022 by the Association of Certified Fraud Examiners (ACFE) Global Study on Occupational Fraud and Abuse, occupational fraud is the most significant and prevalent threat organizations may face. Occupational fraud occurs when an organization's officers, directors, or employees commit fraud against it. It is an internal attack on the organization by the people entrusted with protecting its assets and resources. Since the ACFE began collecting data on occupational fraud cases in 1996, it has documented thousands of instances in which perpetrators stole millions of dollars from their employers.

Forensic accounting investigation is divided into three broad categories: litigation services, investigative services, and expert witness. Forensic accountants should always be experienced, skeptical, thoughtful, independent, and highly knowledgeable within the fields listed. Those in this forensic profession must keep up with changing conditions and adapt. Even if they are not traditional auditors, they must be familiar with auditing standards since they have to cover their exceptional professional capabilities and conventional audit and accounting information.

It can be stated that forensic accounting is now a well-known and in-demand profession. The Enron and WorldCom scandals discussed in previous chapters exposed fraud risks and the possibility that it goes undetected. Despite these negative fraud scenarios, there are accessible solutions, including, to begin, the implementation of an adequate control system, the management of corporate risks, which includes the evaluation of the risk of fraud in the organization, the implementation of crucial anti-

fraud controls, and seeking ways to prevent fraud in a personalized way for each company. The internal control system is adequate if it allows for clear and precise information indication of the leading corporate risk factors, as well as their continuous monitoring and management, in order to ensure factors such as the safeguarding of corporate assets, the efficiency and effectiveness of business processes, the trustworthiness of information supplied to corporate bodies and the market, and compliance with laws, regulations, and the articles of association.

The increasing complexity of business structures and increased expectations for the effectiveness of corporate governance prompted COSO to update the original document several times, most notably the ERM in 2017. The update essentially incorporates all of the main aspects of the original framework and is intended to help organizations create, retain, and realize value while improving their risk management approach. This update removed doubt that risk is fully integrated into the strategic planning process and an organization's performance context. Moreover, rather than being portrayed as a separate topic, risk management is permeated throughout the company to anticipate risk better so that it can be anticipated, with the understanding that change can create opportunities, not just the risk potential.

Although much has been done, it is clear that more needs to be done to prevent scandals like the ones described above. The Sarbanes-Oxley Act of 2002 was enacted to combat fraud, and while it has improved reporting transparency and the independence of public accountants, more needs to be done. Forensic accountants should be used more frequently because there are still a significant number of frauds that go undetected until the victim declares bankruptcy. Fraud prevention and prompt detection are critical.

Cybersecurity is another critical control mechanism that has grown in importance in today's technological world. Recognizing that cybersecurity and internal control

mistakes can have unintended consequences is critical. Businesses should safeguard their stakeholders by preventing fraud. Cybersecurity experts can help prevent, detect, and respond to data theft, cyber intrusions, and other technological vulnerabilities. Similarly, forensic accountants are specially trained and skilled at detecting corporate misconduct, noteworthy trends, financial anomalies, asset misappropriation, and resolving related control weaknesses. Cybersecurity and forensic accounting experts can work closely together to distribute a potent one-two punch in the face of corporate crime.

Lastly, there is an emptiness in the literature of forensic accounting in Italy as it is a practice not yet popularized and recognized in the nation. As explained in the chapter, various bodies form a group to resolve similar issues. However, the figure itself is not considered very common. The leading auditing companies discuss the importance of the forensic accountant, and it could even be said that there is a substantial market advertisement by these companies not only to hire said forensic accountant but also to interest the typical auditor into specializing in this field and obtaining the required certificates. A few university courses and certificates can be taken, even though the university's specialized courses are taught based on the United States system of forensic accounting, and not all the teachings can apply to this nation. There is still a lot that needs to be done in Italy to include and employ this figure which, as in the Anglo-Saxon countries, could only bring indispensable help and positive aspects to the job.

In conclusion, modern times necessitate new accounting tasks and present new challenges, given that the accounting field is the most commonly used by perpetrators or authors of illegal activities. Money laundering, financing terrorism, illicit enrichment, fraud, and corruption, among other things, are driving professional accountant to become more specialized and expert in their field. As a result, forensic accounting is

presented as a viable option for increasing the effectiveness of the work in these difficult times. Furthermore, society expects public accountants to provide necessary security so that terrorist groups cannot finance themselves, let alone use financial systems. As a result, a link can be established between several areas to generate more extraordinary contributions and, this link between forensic analysis and regular accounting has brought to life the role of the forensic accounting investigator, a key auditor without which large-scale fraud schemes would be even more popular today then at the time of the major scandals which shook the whole world.

Bibliography

"2018 Coso Erm Framework: Le Principali Novità." (2020). [2018 Coso Erm Framework: The Main Updates] ANRA. Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali. https://anra.it/it/it/article/874/2018-coso-erm-framework-le-principali-novita.

AICPA. (2009). *"The Guide to Investigating Business Fraud"*. New York, NY: American Institute of Certified Public Accountants, Inc.

Agyemang, Malik, Ken Barker, & Rada Alhajj.(2006). *"A Comprehensive Survey of Numeric and Symbolic Outlier Mining Techniques."* Intelligent Data Analysis 10, no. 6. 521–38. https://doi.org/10.3233/ida-2006-10604.

Ahmed, S.R. (2004). *"Applications of Data Mining in Retail Business."* International Conference on Information Technology: Coding and Computing, Proceedings. ITCC 2004., 2004: 455-459. https://doi.org/10.1109/itcc.2004.1286695.

Alleyne, B.J. & Elson, R.J. (2013). "*The impact of federal regulations on identifying, preventing, and eliminating corporate fraud"*. Journal of Legal, Ethical and Regulatory Issues. 16. 91-106.

Allegrini M., D'Onza G., Mancini D., & Garzella F. (2003). *Le frodi aziendali. Frodi amministrative, alterazioni di bilancio e computer crime (Corporate frauds. Administrative frauds, statement alterations and computer crime)*. 7° Edition. Milan:
Franco Angeli.

Alli R., Nicolaides R., & Russell C. (2018). "*Detecting Advance Fee Fraud Emails Using Self-Referential Pronouns: A Preliminary Analysis."* Accounting Forum 42, no. 1. 78–85. https://doi.org/10.1016/j.accfor.2018.01.003.

Al-Okaily, Manaf, Hamza Mohammad Alqudah, Anas Ali Al-Qudah, & Abeer F. Alkhwaldi. (2022). *"Examining the Critical Factors of Computer-Assisted Audit Tools and Techniques Adoption in the Post-Covid-19 Period: Internal Auditors Perspective."* VINE Journal of Information and Knowledge Management Systems. 31–58. https://doi.org/10.1108/vjikms-12-2021-0311.

Alshurafat, Hashem, Mohannad Obeid Al Shbail, & Ebrahim Mansour. (2021) *"Strengths and Weaknesses of Forensic Accounting: An Implication on the Socio-Economic Development."* Journal of Business and Socio-economic Development 1, no. 2. 135–48. https://doi.org/10.1108/jbsed-03-2021-0026.

Amani, Farzaneh A., & Adam M. Fadlalla. (2017). *"Data Mining Applications in Accounting: A Review of the Literature and Organizing Framework."* International Journal of Accounting Information Systems 24. 32–58.

https://doi.org/10.1016/j.accinf.2016.12.004.

Association of Certified Fraud Examiners. (2022). *"Report To The Nations On Occupational Fraud And Abuse". Global fraud study. ACFE.*

"Audit Risk - Completed." (2019). IAASB. International Auditing and Assurance Standards Board. https://www.iaasb.org/projects/audit-risk-completed.

Axelsen, M., Green, P. & Ridley, G. (2017), *"Explaining the information systems auditor role in the public sector financial audit",* International Journal of Accounting Information Systems, Vol. 24, pp. 15-31.

Banca d'Italia. (2022). *Anti-money laundering*. UIF - Financial Intelligence Unit. Retrieved October 18, 2022, from https://uif.bancaditalia.it/normativa/norm-antiricic/index.html?com.dotmarketing.htmlpage.language=1

Barrett M. J., Enron, (2002). *"Accounting and Lawyers".* Notre Dame Lawyer, pp. 14-20. Available at SSRN: https://ssrn.com/abstract=782365

Barzinji, Zardasht A. Q. (2022). *"The Effect of Forensic Accounting on Fraud Prevention, the Moderating Role Internal Control Effectiveness."* International Journal of Economics, Commerce and Management X, no.1. 213–30. https://doi.org/2348 0386.

Bierstaker, J., Janvrin, D. & Lowe, D.J. (2014), *"What factors influence auditors' use of computerassisted audit techniques?"*, Advances in Accounting, Vol. 30 No. 1, pp. 67-74.

Blois, K. & Ryan, A. (2013) "*Affinity fraud and trust within financial markets",* Journal of Financial Crime, Vol. 20 No. 2, pp. 186-202. https://doi.org/10.1108/13590791311322364

Burg, Dave, Alam Hussain, Richard J. Watson, & EY Global. (2021). "*Cybersecurity: How Do You Rise above the Waves of a Perfect Storm?"* EY. Ernst & Young Global Limited. https://www.ey.com/en_gl/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm.

Carey, C. & Webb, J.K. (2017) *"Ponzi schemes and the roles of trust creation and maintenance",* Journal of Financial Crime, Vol. 24 No. 4, pp. 589-600. https://doi.org/10.1108/JFC-06-2016-0042

"Certified Forensic Computer Examiners." (2022). ISFCE. The International Society of Forensic Computer Examiners. https://www.isfce.com/.

Chartered Global Management Accountant (CGMA), (2013). *"Report From Insight*

to Impact: Unlocking Opportunities in Big Data". Available at:. http://www.cgma.org/Resources/Reports/DownloadableDocuments/From_insight_to_impact-unlocking_the_opportunities_in_big_data.pdf.

Chen, H., Hua, S., & Sun, X. C (2018). *"CEO Age and the Persistence of Internal Control Deficiencies".* Journal of Accounting & Finance. 2158-3625.

"Coso Releases New Guidance: Enabling Organizational Agility in an Age of Speed and Disruption." (2022). COSO. Committee of Sponsoring Organizations. https://www.coso.org/Shared%20Documents/COSO-News-Release-Enabling-Organizational-Agility.pdf?web=1.

Crain, Michael A., William S. Hopwood, Carl Pacini, & George R. Young. (2016). "*Essentials of forensic accounting*." http://www.vlebooks.com/vleweb/product/openreader?id=none&isbn=9781119552260.

Crain, Michael A., William S. Hopwood, Richard S. Gendler, George R. Young, & Carl Pacini. (2015). "*Essentials of Forensic Accounting*." New York, New York: American Institute of Certified Public Accountants inc.

Curtis, M.B. & Payne, E.A. (2014), *"Modeling voluntary CAAT utilization decisions in auditing",* Managerial Auditing Journal, Vol. 29 No. 4, pp. 304-326.

Crumbley, D. L. (2001). *"Forensic Accounting: Older Than You Think",* Journal of Forensic Accounting, S.(2), 181-202.

Crumbley, D. L., Heitger, L. E., & Smith, G. S. (2015). *"Forensic and Investigative Accounting"* (Seventh ed.). Wolters Kluwer.

D'Onza G., Mancini D., & Garzella F. (2003). *"Corporate fraud. Administrative fraud, budget alterations and computer crime."* 7° Edition. Milan: Franco Angeli.

Dellaportas Steven. (2013). *"Conversations with inmate accountants: Motivation, opportunity, and the fraud triangle".* Accounting Forum, 37(1).

Dias, A. P. (2017). *"A more Effective Audit after Coso ERM 2017 or after ISO 31000:2009?"* CEIPDA - Arizona State University. Revista Perspectiva Empresarial, 4(2), 73–82. https://www.semanticscholar.org/paper/A-more-effective-audit-after-COSO-ERM-2017-or-after-Dias/6eca9299517589a664e35d41216b0f95fe385507.

DiGabriele, James A. (2009). *"Implications of Regulatory Prescriptions and Audit Standards on the Evolution of Forensic Accounting in the Audit Process."* Journal of Applied Accounting Research. Emerald Group Publishing Limited. https://www.emerald.com/insight/content/doi/10.1108/09675420910984673/full/html.

Duffield, Grace M., & Peter N. Grabosky. (2001). *"The Psychology of Fraud".* Vol. 199. Canberra, Australia: Australian Institute of Criminology.

Durtschi, C., Hillison W. & Pacini C. (2004). *"The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data."* Journal of Forensic Accounting. R.T. Edwards Inc. http://lycofs01.lycoming.edu/~sprgene/M400/BenfordsLaw.pdf.

"Economic Impact of Cybercrime—No Slowing down Report." (2018). McAfee. McAfee LLC. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf.

El Aziz Hegazy, M. & Kassem, R., (2010*). "Fraudulent Financial Reporting: do red flags really help?"*. Journal of Economics and Engineering, (4), pp.69-79.

"*Enron Scandal - A Series of Financial Wrongdoings That Led to the Collapse of Enron Corporation in 2001."* (2020). Corporate Finance Institute. CFI, May 12. https://corporatefinanceinstitute.com/resources/knowledge/other/enron-scandal/.

"Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA)." (1989). FRASER. Federal Reserve System, August 9. https://fraser.stlouisfed.org/title/financial-institutions-reform-recovery-enforcement-act-1989-firrea-1046.

Fiske, A.P. (2004). *"Relational models theory 2.0",* in Haslam, N. (Ed.), Relational Models Theory: A Contemporary View, Lawrence Erlbaum Associates, Mahaw, NJ, pp. 3-26.

Fokuoh Ampratwum, E. (2009)."*Advance fee fraud "419" and investor confidence in the economies of sub-Saharan African (SSA)",* Journal of Financial Crime, Vol. 16 No. 1. 67-79. https://doi.org/10.1108/13590790910924975

"Forensic Accountant Career Path." (2022). ACFE. Association of Certified Fraud Examiners Inc. https://www.acfe.com/career/career-paths/career-path-accounting/career-path-detail-forensic-accountant.

"Foreign Corrupt Practices Act." (2017). The United States Department of Justice, February 3. https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act.

"Fraud 101: What Is Fraud?" (2022). ACFE. Association of Certified Fraud Examiners. https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud.

"Fraud Examiners Manual: 2022" (2022). ACFE - Association of Certified Fraud Examiners, 3(3). Austin, Texas.

"Fraud Risk Management – Providing Insight into Fraud Prevention, Detection

and Response." (2012). Deloitte Touche Tohmatsu Limited. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/Forensic-Proactive-services/in-fa-frm-noexp.pdf.

Fusaro, P. C. & Ross M. M. (2002). *"What Went Wrong at Enron".* Hoboken, NJ: John Wiley & Sons, Inc.

Gamlath , M. M. S., Ab Yajid, M. S., & Khatibi, A. (2018). *"The New Fraud Triangle Theory - Integrating Ethical Values of Employees".* Retrieved from http://ijbel.com/wp-content/uploads/2018/08/ijbel5_216.pdf

"Generally Accepted Accounting Principles (GAAP) - Guidelines & Policies." (2022). Accounting. https://www.accounting.com/resources/gaap/.

Golden, Thomas W, Skalak, Steven L., Clayton, Mona M., & Pill, Jessica S. (2006). *"A Guide to Forensic Accounting Investigation".* 2. Vol. 2. John Wiley & Sons.

Golden, Thomas W., Skalak, Steven L., Clayton, Mona M., & Pill, Jessica S. (2012). *"A guide to forensic accounting investigation"* (Second). John Wiley & Sons.

Granlund, M., Mouritsen, & J., Vaassen, E. (2013).*"On the relations between modern information technology, decision making and management control".* Internatonal Journal of Accounting Information Systems. 4 (14), 275–277.

Gray, Dahli. (2015). *"Forensic Accounting and Auditing: Compared and Contrasted to Traditional Accounting and Auditing."* American Journal of Business Education. Clute Institute. 6901 South Pierce Street Suite 239, Littleton, CO 80128.

Gray, Dahli, & Clemense Ehoff Jr. (2015). *"Sarbanes-Oxley and Dodd Frank: Then There Was Fraud."* Journal of Business & Economics Research (JBER) 13, no. 1.19. https://doi.org/10.19030/jber.v13i1.9076.

Han, J., Kamber, M., & Pei, J. (2006). *"Data Mining: Concepts and Techniques".* Morgan Kaufmann.

Homer, E.M. (2020)*, "Testing the fraud triangle: a systematic review",* Journal of Financial Crime, Vol. 27 No. 1, pp. 172-187. https://doi.org/10.1108/JFC-12-2018-0136

Hopwood, W., Leiner, J., & Young, G. (2012). *"Forensic accounting and fraud examination"*. Second edition. New York: McGraw-Hill

Howieson, Bryan. (2018). *"What Is the 'Good' Forensic Accountant? A Virtue Ethics Perspective."* Pacific Accounting Review. Emerald Publishing Limited, April 3. https://www.emerald.com/insight/content/doi/10.1108/PAR-01-2017-0005/full/html.

"Internal Audit 2012: A Study Examining the Future of Internal Auditing and the Potential Decline of a Controls-Centric Approach." (2012). PwC . PricewaterhouseCoopers LLP. https://www.pwc.com/sg/en/advisory/assets/publication-internal-audit-2012.pdf.

"Internal Control: A Practical Guide." (1999). KPMG. KPMG International Cooperative.

Johnson, Leighton R. (2014). *"Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response".* Amsterdam, Netherlands: Syngress.

Kaur, Baljinder, Kiran Sood, & Simon Grima. (2022). *"A Systematic Review on Forensic Accounting and Its Contribution towards Fraud Detection and Prevention."* Journal of Financial Regulation and Compliance. Emerald Publishing Limited, June 7. https://www.emerald.com/insight/content/doi/10.1108/JFRC-02-2022-0015/full/html.

Kayvon, Paul J. (2021). *"Playing the Game: Hedge Funds, Brokerage Firms, and Social Media Influencers in the Context of SEC Rule 10b-5 Market Manipulation."* Ohio State University. Moritz College of Law. Ohio State Business Law Journal. Vol. 16. n.1. 37-65, January 1. https://kb.osu.edu/handle/1811/101716.

Khuzami R., & Walsh J., (2009)."*SEC's Failure to Identify the Bernard L. Madoff Ponzi Scheme and How to Improve SEC Performance,"* testimony before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, September 10. http://www.sec.gov/news/testimony/2009/ts091009rk-jw.htm.

KPMG International. (2016). *"Global profiles of the fraudster - Technology enables and weak controls fuel the fraud".* Assets KPMG. Retrieved 2022, from https://assets.kpmg/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf

Lyke B., & Jikling, M. (2002). *"Worldcom: The Accounting Scandal."* Congressional Research Service, August. https://www.everycrsreport.com/files/20020829_RS21253_e7ed921fa695fd4b8a0986316b6cd894a557e163.pdf.

Louwers, Timothy J. (2015). *"The Past, Present, and Future (?) of Crime-Related Forensic Accounting Methodology."* Accounting Research Journal. Emerald Group Publishing Limited, July 6. https://www.emerald.com/insight/content/doi/10.1108/ARJ-04-2015-0047/full/html.

Lowe, D.J., Bierstaker, J.L., Janvrin, D.J. & Jenkins, J.G. (2017), *"Information technology in an audit context: have the big 4 lost their advantage?",* Journal of Information Systems, Vol. 32 No. 1, pp. 87-107.

Lundelius, Charles R. (2011). *"Financial Reporting Fraud: A Practical Guide to Detection and Internal Control".* New York, New York: American Institute of Certified Public Accountants.

Lux, Allen G., & Sandra Fitiani. (2002). *"Fighting Internal Crime Before It Happens."* Information Systems Control Journal 3. 50–51.

Manning, George A. (2005). *"Financial Investigation and Forensic Accounting"* (2nd ed.). Routledge. https://doi.org/10.1201/9781420039061

Manning, George A. (2012). *"Financial Investigation and Forensic Accounting".* (3rd ed). Boca Raton, FL: CRC Press.

Mohd A. (2020). *"Reviewing Enron Scandal".* September 13. Available at SSRN: https://ssrn.com/abstract=3697549 or http://dx.doi.org/10.2139/ssrn.3697549

Mousa, A., (2016). *"Detecting financial fraud using data mining techniques: A decade review from 2004 to 2015",* Journal of Data Science, 14. 553- 570.

Navarrete, Alberto Clavería, & Amalia Carrasco Gallego. (2022). *"Forensic Accounting Tools for Fraud Deterrence: A Qualitative Approach."* Journal of Financial Crime. Emerald Publishing Limited, May 16. https://www.emerald.com/insight/content/doi/10.1108/JFC-03-2022-0068/full/html.

Nigrini, Mark J. (1999). *"I've Got Your Number."* Journal of Accountancy. Association of International Certified Professional Accountants, May 1. https://www.journalofaccountancy.com/issues/1999/may/nigrini.html.

Nigrini, Mark J. (2011). *"Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations".* 1. Vol. 1. Hoboken, New Jersey: John Wiley & Sons Inc.

Nigrini, Mark J. (2022). *"Using Benford's Law to Reveal Journal Entry Irregularities."* Journal of Accountancy. Association of International Certified Professional Accountants, September 1. https://www.journalofaccountancy.com/issues/2022/sep/using-benfords-law-reveal-journal-entry-irregularities.html.

"Oxley News, February 2022." (2022). SOXCPA. Sarbanes-Oxley Compliance Professionals Association, https://www.sarbanes-oxley-association.com/Sarbanes_Oxley_News_February_2022.html.

Panigrahi, P. K. (2006). *"Discovering Fraud in Forensic Accounting Using Data Mining Techniques"*, The Chartered Accountant, April, New York. 1426- 1430. http://220.227.161.86/102541426-1430.pdf

Pedneault, Stephen, & Frank Rudewicz. (2012). *"Forensic Accounting and Fraud Investigation for Non-Experts",* 3rd Edition. Thirded. John Wiley & Sons.

Perri, Frank S., & Richard G. Brody. (2011). *"Birds of the Same Feather: The Dangers of Affinity Fraud."* Journal of Forensic Studies in Accounting and Business 3, no. 1. 33– 46.

Petrick, J.A. & Scherer, R.F. (2003). *"The Enron Scandal and the Neglect of Management Integrity Capacity",* American Journal of Business, Vol. 18 No. 1, 37 -50. https://doi.org/10.1108/19355181200300003

Pogliani, Giuseppe, Nicola Pecchiari, M. Mariani, & Donato Masciandaro. (2012). *"Frodi Aziendali: Forensic Accounting, Fraud Auditing E Litigation".* Milano, Italy: Egea,

PricewaterhouseCoopers. (2016). *"Global State of Information Security Survey."* PwC. PricewaterhouseCoopers. https://www.pwc.com/sg/en/publications/global-state-of-information-security-survey-2018-sg.html.

"Public Law 107–204 107th Congress an Act." (2002). Congress Government. United States Congress. https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf.

Pwc. (2022). PWC's Global Economic Crime and Fraud Survey 2022. PwC. Retrieved July 29, 2022, from https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

Rechtman, Yigal. *"The Past, Present, and Future of Forensic Accounting."* The CPA Journal. New York State Society of CPAs, April 7, 2020. https://www.cpajournal.com/2020/04/10/the-past-present-and-future-of-forensic-accounting/.

"Recordkeeping and Internal Controls Provisions Section 13(b) of the of the Securities Exchange Act of 1934." (2003). SEC. U.S. Securities and Exchange Commission. https://www.sec.gov/spotlight/fcpa/fcpa-recordkeeping.pdf.

Sauer R. C. (2010). *"Why the SEC Missed Madoff,"* Wall Street Journal, July 17.

"Sarbanes-Oxley Act of 2002", (2002). United States Security and Exchange Commission. 2002: 101-1107.

Schroeder, S.B, Skolnik, b. & Strom R. (2022). *"Chapter 11- Bankruptcy." Bloomberg* Law. The Bureau of National Affairs, October 10.

https://pro.bloomberglaw.com/brief/chapter-11-bankruptcy/.

Siew, E.G., Rosli, K. Yeow, P.H. (2020), *"Organizational and environmental influences in the adoption of computer-assisted audit tools and techniques (CAATT) by audit firms in Malaysia",* International Journal of Accounting Information Systems, Vol. 36, p. 100445.

Silverstone, Howard, Michael Sheetz, Stephen Pedneault, & Frank Rudewicz (2012). *"Forensic Accounting and Fraud Investigation for Non-Experts"*. Thirded. John Wiley & Sons Inc.

Singleton, T., & Singleton, A. (2010). *"Fraud auditing and forensic accounting"*. Hoboken: John Wiley & Sons. Inc.

Singleton, T. W., Singleton, A. J., Bologna, G. J., & Lindquist, R. J. (2006). *"Fraud auditing and forensic accounting"*. Thirded. Hoboken, NJ: John Wiley & Sons.

Skalak Steven L., Thomas W. Golden, Mona M. Clayton & Jessica S Pill. (2011). *"A Guide to Forensic Accounting Investigation"* (2nd ed). 2nd ed. Hoboken: John Wiley & Sons. http://www.books24x7.com/marc.asp?bookid=34732. 2012.

Surendranath R. Jory, & Mark P. (2011). *"Ponzi Schemes: A Critical Analysis",* Journal of Financial Planning. Online, Available at SSRN: https://ssrn.com/abstract=1894206

Telpner, Zeph, & Michael S. Mostek. (2003). *"Expert Witnessing in Forensic Accounting: A Handbook for Lawyers and Accountants"*. Boca Raton, Florida: CRC Press.

Thabit, Thabit. (2019). *"Determining the Effectiveness of Internal Controls in Enterprise Risk Management Based on COSO Recommendations."* SSRN. nternational Conference on Accounting, Business Economics and Politics. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3401199.

"The Relationship between Forensic Accounting & Cybersecurity." (2020). Eide Bailly. Eide Bailly LPP. https://www.eidebailly.com/insights/articles/2020/3/the-relationship-between-forensic-accounting-and-cybersecurity.

Tiwari, Reshma Kumari, & Jasojit Debnath. (2017). *"Forensic Accounting: A Blend of Knowledge."* Journal of Financial Regulation and Compliance. Emerald Publishing Limited, February 13. https://www.emerald.com/insight/content/doi/10.1108/JFRC-05-2016-0043/full/html.

Turba, E., Aronson, J.E., Liang, T.P., & Sharda, R. (2007). "*Decision Support and*

Business Intelligence Systems". Pearson Education. volume 8.

Udeh, Ifeoma. (2012). "*An Investigation of Internal Control Related Frauds and Auditor Litigation: Pre- and Post- Sarbanes-Oxley, Section 404."* Scholar's Compass. Virginia Commonwealth University. https://scholarscompass.vcu.edu/cgi/viewcontent.cgi?article=3735&context=etd.

Wagner, V. (2004). *"Nigerian scam has new twist",* Credit Union Magazine, Vol. 70 No. 9. 70- 2.

Webster, J., & Drew, J. M. (2017). *"Policing advance fee fraud (AFF): Experiences of fraud detectives using a victim-focused approach".* International Journal of Police Science & Management, 19(1). 39–53. https://doi.org/10.1177/1461355716681810

Wells, Joseph T. (2013) *"Corporate Fraud Handbook: Prevention and Detection".* Fourth edition. Hoboken, NJ. John Wiley & Sons inc.

Wells, Joseph T. (2014). *"Principles of Fraud Examination".* Fourth edition. Hoboken, New Jersey: John Wiley & Sons inc.

"What is accounting?" (2022). Accounting Verse. Retrieved June 9, 2022, from https://www.accountingverse.com/accounting-basics/what-is-accounting.html

Williams, J.W. (2013) *"Regulatory technologies, risky subjects, and financial boundaries: governing 'fraud' in the financial markets".* Accounting Organizations and Society. 38 (6), 544– 558.

Wilson, S. (2022). *"How Forensic Accountants Partner with Cybersecurity Teams When a Data Breach Occurs: CPA 2022 Requirements by State: CPA Exam and Accountant Education."* Accounting Education. Wiley University Services. https://www.accountingedu.org/how-forensic-accountants-partner-with-cybersecurity-teams-when-a-data-breach-occurs/.

Wisner D. L., & Brown B.A. (2015). *"Corporate Toxicity: The WorldCom/MCI Scandal."* Handle Proxy. The Brandy A Brown Lab Website, February 18. http://hdl.handle.net/10150/345957.

Wolfe, David T., & Dana R. Hermanson. (2004). *"The Fraud Diamond: Considering the Four Elements of Fraud."* CPA Journal 74.12. 38 -42.

Xiao, M., Xiaoli, & H., Gaojin, L. (2010). *"Research on application of data mining technology in financial decision support system".* Proceeding of the International IEEE Conference on Information Management, Innovation Management and Industrial Engineering (ICIII), Kunming, China November. 381 –384. 10.1109/ICIII.2010.572.

Yamanishi, Kenji, Jun-ichi Takeuchi, Graham Williams, &Peter Milne. (2004). *"On-Line Unsupervised Outlier Detection Using Finite Mixtures with Discounting Learning Algorithms."* Data Mining and Knowledge Discovery 8, no. 3. 275 –300. https://doi.org/10.1023/b:dami.0000023676.72185.7c.

Yue, Dianmin, Xiaodan Wu, Yunfeng Wang, Yue Li, & Chao-Hsien Chu. (2007). *"A Review of Data Mining-Based Financial Fraud Detection Research."* International Conference on Wireless Communications, Networking and Mobile Computing, 2007, 5519–22. https://doi.org/10.1109/wicom.2007.1352.

Zack, Gerard M. (2013). *"Financial Statement Fraud: Strategies for Detection and Investigation".* Hoboken, New Jersey: John Wiley & Sons inc.

Zhang, D., & L. Zhou. (2004). *"Discovering Golden Nuggets: Data Mining in Financial Application."* IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews) 34, no. 4. 513– 22. https://doi.org/10.1109/tsmcc.2004.829279.