Expert Systems With Applications 207 (2022) 117981

Contents lists available at ScienceDirect

Expert Systems With Applications

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

Detection of shell companies in financial institutions using dynamic social network

José-de-Jesús Rocha-Salazar [a,*], María-Jesús Segovia-Vargas [b], María-del-Mar Camacho-Miñano [c]

[a] Faculty of Statistical Studies, Complutense University of Madrid, Madrid, Campus, Moncloa, Street, Puerta de Hierro 1, Postal Code 28040, Spain
[b] Financial & Actuarial Economics & Statistics Department, Faculty of Economics and Business Administration, Complutense University of Madrid, Madrid, Building 5, Office 107. Campus, Somosaguas, Pozuelo de Alarcón Postal Code 28223, Spain
[c] Accounting and Finance Department, Faculty of Economics and Business Administration, Complutense University of Madrid, Madrid, Building 6th. Office 63. Campus, Somosaguas, Pozuelo de Alarcón, Postal Code 28223, Spain

ARTICLE INFO

Keywords:
Shell companies
Social networks
Crime
Dynamic
Detection

ABSTRACT

Shell companies work in financial interaction with other companies to commit several crimes such as concealing resources of illicit origin (money laundering), tax fraud (tax evasion), corruption, bribery, and drug trafficking, among others. This interaction can be represented by a set of nodes and connections that show the multiple relationships between entities over time. The current article proposes to detect transactions related to shell companies in financial systems, using legal person attributes and incorporating self and group comparisons into dynamic social networks. The months of June 2019, September 2020, and November 2021 are taken as evaluation periods to test the proposed methodology. Our methodology performs better than the traditional rules method, yielding balanced accuracies and true positive rates above 0.9 and 0.85, respectively. The false-positive rate was also lower in the proposed model than in the rule system for most evaluation periods. The latter translates into a reduction in costs by compliance investigations.

1. Introduction

In October 2021, the International Consortium of Investigative Journalists (ICIJ) launched a global investigation called the “Pandora Papers”, seeking to know the veiled world of offshore finance, a system often used to hide wealth from tax authorities, creditors, and criminal investigations. The 2016 “Panama papers” also revealed hidden wealth using shell companies in several countries. Thousands of shell companies have been recently discovered for tax avoidance purposes worldwide[1]. To the best of our knowledge, this paper is the first to detect transactions related to shell companies in financial systems using dynamic social networks.

A shell company is any legal person that can be legitimately incorporated but with no independent operations, significant assets, ongoing business activities, or employees (Aggarwal & Dharni, 2020; Force, 2018). The OECD defines it as a firm formally registered, incorporated, or otherwise legally organized in an economy but does not conduct any operations other than in a pass-through capacity. Some shell companies are created for legal purposes, for example, financing foreign operations, investing in overseas capital markets, or easing transfers of assets. Despite lawful purposes, criminals use them to commit different crimes taking advantage of the lack of beneficial ownership disclosure. The beneficial owner is the individual who benefits from the activity of the shell company. In most countries, the regulation does not need to reveal the identity of the beneficial owners to create a company. Still, only a legal representative and a physical address are required. In a shell company, the chosen legal representative rarely has a relationship with the beneficial owner and the company and may even act as a representative of other shell companies (Vail, 2018). This company’s environment makes them the ideal structure to commit crimes such as tax

* Corresponding author.
E-mail addresses: jorocha@ucm.es (J.-d.-J. Rocha-Salazar), mjsegovia@ccee.ucm.es (M.-J. Segovia-Vargas), marcamacho@ccee.ucm.es (M.-d.-M. Camacho-Miñano).

[1] International Consortium of Investigative Journalists. "Pandora Papers: An offshore data tsunami." Accessed October 4, 2021. The Pandora Papers information – the 2.94 terabytes in more than 11.9 million records – comes from 14 providers that offer services in at least 38 jurisdictions. The 2016 “Panama Papers” investigation was based on 2.6 terabytes of data in 11.5 million documents from a single provider.

https://doi.org/10.1016/j.eswa.2022.117981
Received 16 October 2021; Received in revised form 20 May 2022; Accepted 23 June 2022
Available online 29 June 2022

fraud, bribery, corruption, drug trafficking, money laundering, mortgage, bankruptcy fraud, terrorist financing, and prohibited nuclear technology movement (Allred, Findley, Nielson & Sharman, 2017; Cooley, Heathershaw & Sharman, 2018; Jancsics, 2017; Tiwari, Gepp & Kumar, 2020).

The criminal actions of shell companies represent a problem for the countries' economies and governments. Some of their adverse effects are control loss of the country's economic policies, economic distortion, investment instability and less collection of taxes (Rocha-Salazar, Segovia-Vargas & Camacho-Miñano, 2021). For this reason, their detection and elimination have entered the agenda of the G20 member countries and intensified since the well-known case of "Panama Papers" (Schuknecht & Siegerink, 2021). The Panama Papers leak in 2016 gave rise to evidence of its use for tax evasion and concealment of assets of doubtful origin where politicians, entertainment celebrities, corporate leaders, and heads of state were involved. Some examples of notorious cases are the senior adviser of the Canadian prime minister, Justin Trudeau, who was engaged in millions of dollars to the Cayman Islands through his family business and a trust fund in the mentioned country (The Guardian, 2017a). Also, the case of a British former Treasury minister sheltered a millionaire family fortune from taxes using a trust fund in the Bahamas in which he was the beneficiary (The Guardian, 2017b). And the case of Nicaraguan President, Arnoldo Alemán used shell companies to divert public resources to personal accounts (Jancsics, 2018). Furthermore, the "Pandora Papers" investigation has many similarities with the "Panama papers" but more information related to tax avoidance. Thus, it is shown that the existence of shell companies is not a national but a global problem.

In the financial sector, institutions have strengthened their internal regulation to comply with a more complete "Know Your Customer" (KYC) policy on their legal persons. This aim is to track the beneficial ownership and source of resources of any transaction. Unfortunately, despite the best efforts, the intellectual actors of shell companies use different intermediaries and third parties who carry out paperwork and transactions on their behalf, hampering the detection task. Adding to this, the detection problem increases when the resources are distributed into different internal and external accounts in the financial systems through a complex network of connections among legal persons.

The financial resources managed or moved by the shell companies, in most cases, are inserted into financial institutions through transactions characterized by a set of attributes. These attributes, when combined, can show patterns seen in shell companies' crimes. Our article takes advantage of transactional features and the natural interaction among shell companies to propose using self and group comparisons into dynamic social networks to detect their criminal activity. Data from a Mexican institution is used to test this methodology. Mexico is a member of the G20 countries and has a well-documented history of illegal acts with shell companies involved. On one side, it has the apocryphal invoice market inserted in the formal economy, usually operated by shell companies (Cruz-Pérez, 2020). On the other hand, there is plenty of evidence of acts of corruption committed between state rulers, government institutions, organized crime, and shell companies to divert public funds and launder money (Secretariat of Finance and Public Credit, 2019).

After this introduction, the article is structured as follows. Section 2 reviews the relevant literature, exposes gaps and shows the contributions. Section 3 explains the proposed methodology. Section 4 includes the sample and variables used in the study. The main model results from testing our idea appear in Section 5. The general conclusions appear in Section 6.

2. Literature review, limitations, and contribution

2.1. Shell companies' detection

The detection of shell companies and their beneficiaries represents a challenge for OECD countries and their governments that have established increasingly rigorous multilateral tax transparency standards and more comprehensive Know Your Customer (KYC) policies in the financial institutions (Allred et al., 2017). Despite this, the globalization of trade and technological advances seem to have favoured the creation and operation of shell companies. An example of this is observed in Mexico, which took advantage of technology to implement a digital billing scheme to improve the security of the authenticity of tax receipts. However, the same technology allowed the increase of deductions through false invoices where shell companies were involved (Barajas, Campos, Sobarzo & Zamudio, 2011; Cruz-Pérez, 2020). The literature related to the detection of shell companies is scarce. A first study is by Pawde, Apte, Palshikar and Attar (2018), which used synthetic data to simulate the collusion-based malpractices of shell companies. They incorporate this proposal into Banking Transaction Simulator (BTS) to generate data sets and tackle the problem of shell-set detection. Then, Luna, Palshikar, Apte and Bhattacharya (2018) simulate banking transactions to detect shell companies using an anomaly detection algorithm. A third study is Joaristi, Serra and Spezzano (2019), which developed an innovative algorithm called "Suspiciousness Rank Back and Forth" (SRBF) that computes a suspiciousness score for each person/company based on their connections in a targeted social network. They apply the algorithm to ICIJ[2] Offshore Leaks Database to detect offshore leak networks. Later, Aggarwal and Dharni (2020) prove the validity of Benford's Law to discriminate between the shell and non-sell companies using financial statement information. Finally, Tiwari, Gepp and Kumar (2021) propose using a hybrid statistical approach to detect money laundering shell companies. They analyze data of 208 limited companies from open sources in the UK, along with 205 cases of other companies that may be involved in illicit activities. After applying distinct classification models for the combination of graph algorithms, they achieve an accuracy of prediction that ranges from 0.8817 to 0.9785.

Despite the efforts, some limitations are observed in these investigations regarding the scope of our study. The first and second studies have a weak point: their applications use simulated data instead of real. The third article is applied explicitly to the ICIJ Offshore Leaks Database. Although it is an environment where shell companies interact, it is not applicable and specialized to the financial institution setting. The next one is entirely based on financial statements whose information can fluctuate out the normal pattern in economic crisis, and market variations without being necessarily a shell company. It also leans on the reliability of calculated metrics from financial statements provided by the company, leaving aside other mechanisms such as having the same shareholders, duplicate addresses, virtual offices, etc. The last one tests the proposed methodology usefulness using a sample of 205 entities that are not confirmed to be money laundering shell companies. Furthermore, it takes data from open sources that are not necessarily related to the financial sector.

2.2. Action mechanisms of shell companies.

The use of shell companies to commit crimes is based on specific techniques and methodologies. In this section, we explain the main action mechanisms implemented by shell companies to execute crimes in financial systems. These mechanisms serve as elements that allow tracking transactions related to these structures.

2.2.1. Money laundering

Criminals use a variety of mechanisms and techniques to conceal the origin and ownership of illicitly obtained resources. According to Financial Action Task, Force (2014, 2018), this overshadowing is done

[2] The International Consortium of Investigative Journalists is a global network of more than 190 investigative journalists in more than 65 countries who collaborate on in-depth investigative stories.

mainly through shell companies in financial systems. Money laundering in financial systems has 3 phases: placement, layering and integration. In the placement phase, money is introduced into financial systems mainly in cash through a series of deposits to shell companies. Then, the money is transferred to other accounts in the layering stage, usually interconnected. These accounts can correspond to shell companies with directors and shareholders in common, low-key young shareholders or being one the provider of another (Luna et al., 2018). This complex network of companies created by a money-laundering agent is aimed to hide the source and beneficiary identity. In the layering process, the resources deposited in the origin accounts have a short duration. Finally, in the integration phase, the money is legitimately used in activities characteristic of money laundering agents, such as real estate investments, donations to charities, leasing of real estate, investment in metals, jewellery, and watches, and allocation of resources to public projects (Secretariat of Finance and Public Credit, 2016).

2.2.2. Tax evasion

Shell companies are often used for tax evasion. An example of this is seen in the ICIJ Offshore Leaks Database, which shows a complex network of companies, people and governmental organizations involved with offshore companies in tax havens. This database is formed for the four networks known as Panama Papers, Paradise Papers, Offshore Leaks, and Bahamas Leaks. The pattern observed in these documents for tax evasion is the establishment of shell companies in bank accounts assigning several legal representatives. These legal representatives manage the accounts for the benefit of the main owner (Joaristi et al., 2019). In a complex network, the money is moved to tax havens through bank transactions between national and international shell companies.

Another tax evasion scheme used by shell companies is the apocryphal invoice market. In countries like Mexico, this market has a well-defined supply and demand and is inserted in the real economy. Apocryphal invoices arise from simulated financial transactions, that is, operations that do not involve the real exchange of goods and services. The interaction unfolds as follows. A shell company simulates the sale of an asset to another shell or formal company using an invoice. The latter pays the provider for the transaction mentioned in the invoice through a bank transaction. Later, the supplier shell company returns an amount of money equal to the invoice amount minus a discount percentage. This discount percentage is the profit of the shell company that generates simulated operations. The formal company uses the apocryphal invoice to deduct taxes. In addition to deducting taxes, the receiving shell company can be involved in another interaction where it acts as a generator of apocryphal invoices to generate more profit. For formal companies, the cycle ends when they can deduct taxes on each purchase. In the case of shell companies, these can be related through endless cycles of buying and selling false invoices (Barajas et al., 2011; Cruz-Pérez, 2020). When the authority manages to realize their existence, they have already disappeared. An essential characteristic of shell companies emerges, which is their short duration, two years on average for Mexico. Another feature is that they tend to pay little taxes and have high profits compared to other companies with similar assets.

2.2.3. Corruption and bribery

Approximately 70% of large-scale corruption cases are related to shell companies for identity concealment (Pacini, Hopwood, Young & Crain, 2018; Nielson & Sharman, 2022). The use of shell companies in acts of corruption and bribery is closely related to the government. Politicians and state authorities tend to use shell companies as vehicles to divert public resources to personal accounts. They negotiate diverse contracts for public and social projects with a complex network of shell companies, making them appear legal (Jancsics, 2018). Afterward, the diversion of resources is executed through bank transfers between the government entity and the network of shell companies that conceal the identity of the primary beneficiary.

An alarming example of the conspiracy between the government and shell companies occurred in Mexico in 2015. The government of the state of Yucatán transferred 158 million Mexican pesos (approx. 7.9 million USD) to shell companies that apparently provided study services on severe diseases and other services in the health sector (Avendaño & Chávez, 2019; Secretariat of Finance and Public Credit, 2019). Another example of complicity is that which occurs in electoral campaigns where candidates make a series of shell companies available to receive donations. A recent example of this happened in the United States with the shell company named "Essential Consultants LLC" established by President Trump's lawyer Michael Cohen to receive donations in return for insights about the new president (Jancsics, 2018). These transfers between government and shell companies are frequently carried out through bank transactions that allow their tracking and detection.

2.2.4. Drug trafficking and cartels

The criminal groups dedicated to the drug trade find in the shell companies adequate vehicles to move and conceal the resources from drug trafficking. Drug trafficking cartels in Mexico usually create shell companies with the same addresses and the same legal representative to carry out million-dollar transactions that do not coincide with the tax return to the treasury. In Mexico, these companies are mostly related to the real estate sector, buying/selling jewellery, and electronic items. Their addresses do not coincide with these declared economic activities, putting in their place private home addresses or using virtual offices. Once the cartels carry out the corresponding transactions, the shell companies disappear shortly before the tax authority realizes the illicit origin of the resources (Secretariat of Finance and Public Credit, 2016).

2.2.5. Financial crimes

Shell companies are perfect means to carry out some financial crimes such as loan fraud and identity theft (Nielson & Sharman, 2022). The complex network that can be formed with multiple legal representatives and the lack of knowledge of the identity of the principal beneficiary ease these crimes. When a legal person wants to acquire a loan (such as a mortgage loan or business loan), the financial institution asks for certain documents to confirm the capacity to pay and reliability in fulfilling the contract. Usually, these documents are the balance sheet, income statement, and records of incorporation to verify the tenure of the company and its economic activity. In many cases, when these requirements are not met, legal entities resort to creating shell companies that satisfy the credit conditions. Once the credit is granted, the shell company disappears shortly before the financial institution discovers the falsification of the financial statements (FFIEC, 2009; Singh, 2010). In the same way that financial statements are falsified for a shell company, the legal representative's identity can also be subject to forgery to obscure their identity.

2.2.6. Proliferation financing

In some cases, shell companies are used in conjunction with shipping companies to finance prohibited nuclear technology and the development of suspect nuclear programs. Complex networks of shell companies are formed to exchange dual-use goods (for example, pressure transducers) that serve both civil and military purposes. Transactions are formalized in financial institutions and the network is adequate to conceal the identity of the end user. In these cases, the revision of the economic activity of the legal entities, countries under sanctions and the type of goods traded are vital elements for detecting this activity (Ruehsen & Spector, 2015).

2.3. Contributions

From the literature review described in section 2.1, the following gaps are identified:

a. There is a lack of studies applied to financial systems to detect shell companies. The few ones that exist use simulated data rather than real.
b. The proposed methodologies have been limited to analysing transactions or financial statement information. There is no exploration of other action mechanisms implemented by shell companies, such as false declared addresses, operations with the government, shareholders in common, virtual office possession and other means described in section 2.2.
c. The interaction of shell companies with others in financial systems shows patterns that have not been analyzed. Addresses, shareholders and legal representatives in common with other companies are mechanisms observed in their activity. Also, a low sense of financial relation is present in the interaction. In other words, why does a legal person dedicated to real estate sales make frequent transactions with another dedicated to the jewellery and metals market?
d. The previous studies that implemented network or graphs techniques for detecting shell companies did not contemplate the dynamic/variations of interactions over time. Analyzing these variations may allow better discrimination between suspicious and non-suspicious behaviors.

With the aim of fulfilling these gaps, we propose an innovative methodology with the following contributions:

a. The proposed technique is tested using real transaction attributes of legal persons from a financial institution in Mexico.
b. The model incorporates not only variables related to transactions amounts or metrics from financial statements, but also other action mechanisms observed in shell companies' crimes described in section 2.2. These are the economic activity, whether the clients are politically exposed, whether the legal person's operability is according to their assets, operations with the government, shareholders' age, whether the declared address coincides with the economic activity, virtual offices possession, tenure, and permanence of deposited resources.
c. It also includes a mechanism that emerges from the interaction of two legal persons, such as having addresses, shareholders and legal representatives in common, and whether the financial relation makes sense.
d. The current study contributes to incorporating the self and group comparison on dynamic social networks to consider the interaction variations over time. As mentioned in Rocha-Salazar et al. (2021), financial abnormal behavior can be detected through these two types of comparisons. The self-comparison is incorporated by contrasting the current connection intensities of the legal person pairs with the dynamics of their past intensities. The group-comparison is implemented within the connection intensity calculations and through an optimal risk threshold.

3. Methodology

3.1. Social networks and applications

The act of shell companies in financial institutions implies the interaction of people and companies through financial transactions at the national or international level. This interaction makes social networks ideal for detecting suspicious activities and links.

A social network is a finite set of vertices and defined connections between them. Vertices can represent people, companies, products, and any group of entities on which relationships can be defined. Connections, also known as edges, represent the type of relationships between vertices. In the case of financial institutions, these relationships can be the amount and frequency of transactions between clients, the number of features in common between two natural or legal entities, and the direction of the flow of transactions between two accounts. Formally a social network (SN) consists of a finite nonempty set of vertices $V = \{v_1, v_2, ..., v_n\}$ joined by a finite nonempty set of edges $E = \{e_1, e_2, ..., e_m\}$ being defined as $SN = (V, E)$ (Tabassum, Pereira, Fernandes & Gama, 2018). Thus, the order and the size of a social network are defined analogously to that of a graph as the number of vertices $|V| = n$ and the number of edges $|E| = m$, respectively (Diestel, 1990). The maximum number of edges/connections for an undirected social network will be $\frac{n(n-1)}{2}$ and $n(n-1)$ for the directed one.

In prior literature, the application of social networks to detect financial crimes with positive results is observed in a few studies. Fronzetti and Remondi (2016) implement social networks in the factoring business and their traditional centrality metrics such as in-degree, out-degree, all-degree, closeness, and betweenness centrality to detect money laundering cases. Tang, Barbier, Liu, and Zhang (2010) incorporate social networks to detect online financial crime through the flow of transactions between accounts. The aim is to focus on an unusual number of links/transactions to certain nodes/accounts. Later, Singh and Best (2019) incorporate visualization techniques like directed social networks to detect banking transactions related to money laundering. They represent the transaction flows between bank accounts through nodes and edges intending to find unusual patterns visually. A comprehensive and vast literature review of social network applications in crimes that are not necessarily financial can be found in Bright, Brewer and Morselli (2021).

3.2. Proposed methodology

The clients of a financial institution can be classified into two large groups: natural persons and legal persons. Natural persons are individuals with the capacity to assume obligations and exercise rights. Legal persons are entities with legal representatives commonly called "corporations". Although natural persons can relate to shell companies through financial transactions, they cannot be shell companies themselves. The possibility of being a shell company is present only in legal persons (Quintana-Adriano, 2015). This article proposes to take the legal persons of the financial institution as vertices of the social network. Most social network applications establish vertices and edges that define relationships in cross-sectional data. The relationships between many vertices (individuals, companies, products, etc.) are defined without considering the social variations that may exist over time. Little studies consider certain variations. Morselli and Petit (2007) analyze the evolution of the drug importation network and observe how the centralization of the network and node status change according to the law-enforcement targeting over time. Morselli (2009) explains how the variation in different centrality measures can be incorporated to better analyze important patterns in organized crime. The changing/dynamic aspect of criminal networks is an intrinsic feature that cannot be ignored. Criminals are intelligent entities that adapt to new laws and seek new methods of committing crimes. Their risk factors such as age, source of income, and economic activity are constantly changing. For example, in financial systems, we can define a directed connection between two legal entities A and B, if there are financial transactions from A to B. In a certain period, the transaction amount from person A to person B may be more significant than from B to A. Later, the transaction amount may be more significant from B to A than from A to B or simply the relationship between A and B disappears because there are no more transactions between them. As another example, a connection between two legal entities can be considered suspicious because their legal representatives are currently politically exposed, but later, they may cease to be political or become just natural persons.

The proposed methodology in this study considers the social variations over time introducing the concept of dynamic social network that we represent as $\{(V_t, E_t)\}_{t=1}^{T}$, where $V_t = \{v_{t,1}, v_{t,2}, ..., v_{t,n}\}$ and $E_t = \{e_{t,1}, e_{t,2}, ..., e_{t,n}\}$ for $t = 1, 2, ..., T$. In this way, the result is a set of social networks from its application in longitudinal data, this is, repeated ob-

servations of the same variables over a period. The number of vertices, edges and nature of the relationships will change from one network to another. Most of the social network's applications mentioned in section 3.1 have used the centrality measures to detect suspicious activity. These centrality measures provide information on which elements are essential and central in the spatial distribution of the network (Das, Samanta & Pal, 2018). In the context of shell company activity, the nature of the interaction between peers that own a set of risk factors is more relevant than its spatial distribution characteristics. Experience has shown that there are legal entities with large flows of incoming and outgoing transactions without being confirmed as shell companies. Often, this volume of transactions is related to the nature of the economic activity that enables one to be the provider of goods to the other. It is also possible to have a high number of transactions between a defined group of legal entities perceived in the network as dense zones without confirming any shell company activity. These dense areas indicate high transnationality due to being in the same geographic areas or related economic activities. Cases have also been observed of legal entities that have only had a single interaction over time, with a usual number of incoming and outgoing transactions, and they turn out to be shell companies with addresses and legal representatives in common. Therefore, the proposed methodology and considering social variations over time focus on the risk of peer interaction. The interaction risk is determined by incorporating self-comparison and group-comparison into the social network dynamic.

3.2.1. Methodology process

Legal persons possess "k" mutable attributes that under specific values make them more likely to be a shell company. The set of attributes for a certain legal person "i" in the period "t" will be denoted as $A_t^i = \left\{a_{t,1}^i, a_{t,2}^i, ..., a_{t,k}^i\right\}$. An undirected connection between two legal entities "i", "j" will be defined if there is at least one transaction from "i" to "j" or from "j" to "i". Thus, the final network structure will be made up of unique pairs of legal entities connected by the presence of at least one transaction between them.

Once the vertices and edges are defined, we propose the following methodology that can be programmed as an expert system:

1. Risk metrics assignation: Risk metrics are assigned to the legal person's attributes according to the expert judgment of compliance and risk committees of the institution. Expert judgment is based on years of experience in financial crime analysis, the report Secretariat of Finance and Public Credit (2016), and study cases explained in Force (2014) and Force (2018). Thus, the assigned risk metrics will be consistent with the action mechanisms described in section 2.2. The assigned risk metrics for a legal person "i" in time "t" would be denoted as the vector:

$$(r_{t,1}^i, r_{t,2}^i, ..., r_{t,k}^i) \in R^k \text{ for the attributes } 1, 2, ..., k \quad (1)$$

2. Connection intensity calculation: In this study, the connection intensity is the crucial element in identifying suspicious activity. For its calculation, the risk metrics of two connected legal entities "i", "j" in the period "t" are added as it is shown below.

$$(r_{t,1}^i + r_{t,1}^j, r_{t,2}^i + r_{t,2}^j, ..., r_{t,k}^i + r_{t,k}^j) \quad (2)$$

The sum is chosen intuitively, assuming that the total risk of the connection will be the aggregate risk of the legal persons involved. For example, the interaction of two legal persons with politically exposed representatives, virtual offices and addresses in common will be riskier than an interaction where these characteristics are not met, keeping constant the rest of the attributes.

Once the sum vector has been obtained, its elements are subjected to a function $G: R^k \rightarrow R$ that generate a real number. Where this real number is the connection intensity between two legal persons "i", "j" in the period "t",

$$I_t^{i,j} = G(r_{t,1}^i + r_{t,1}^j, r_{t,2}^i + r_{t,2}^j, ..., r_{t,k}^i + r_{t,k}^j) \quad (3)$$

The function can have any structure and give any treatment to the arguments. The only condition is that resulting intensities are increasing concerning the attributes risk sums.

Rocha-Salazar et al. (2021) establish that financial crime is a form of abnormal pattern in comparison to the common group behavior. Larik and Haider (2011) define an abnormality indicator that incorporates the deviation (Euclidean distance) of transaction amount and the frequency of similar types of transactions from the cluster centroid to the client belongs. The greater the deviation from the centroid, the greater the abnormality indicator. Following a similar logic, we can define a function that considers the deviation of the sum risks of the connections with respect to the group's mean by attribute. These standard deviations will represent the weights of the sum risks of the attributes to calculate the connection intensities in time "t". For legal persons "i", "j" the connection intensity will be:

$$I_t^{i,j} = \frac{\sigma_{t,1}(r_{t,1}^i + r_{t,1}^j) + \sigma_{t,2}(r_{t,2}^i + r_{t,2}^j) + ... + \sigma_{t,k}(r_{t,k}^i + r_{t,k}^j)}{\sum_{a=1}^{k} \sigma_{t,a}} \quad (4)$$

Where $\sigma_{t,1}$ is the standard deviation of the risk sums for attribute 1, $\sigma_{t,2}$ for attribute 2 and so on until attribute k in time "t". In this way, the more dispersed the risk sums respect to the group mean, the greater their contribution to the resulting connection intensity. Defining the connection intensity as mentioned above allows the group-comparison to implicitly represent the interaction of all the risk attributes in a single number.

3. Setting of the self-comparison: Here is where past social networks dynamics are considered. For the self-comparison we introduce the concept of "evaluation period". The evaluation period "T" is the most recent month, quarter, semester, or any other period where the model is run for task detection. The individual comparison is carried out by contrasting the intensities of the evaluation period and the intensities of the past social networks. In this way, for each pair of legal entities "i", "j" connected in the evaluation period "T" there will be a time series of intensities in the following way:

$$\{I_{T-p}^{i,j}, I_{T-(p-1)}^{i,j}, ..., I_{T-1}^{i,j}\} \quad (5)$$

Where "p" is the number of periods used to define the normal/expected behaviour of the legal persons. The weighted moving average of the time series above will be calculated to define the expected intensities in period "T". The weights will be increasing probabilities such that the old intensities have lower weights, and the newer ones have higher weights. This configuration is established following the logic that the most recent interactions are more likely to remain in the evaluation period.

$$I_{T_{expected}}^{i,j} = w_p I_{T-p}^{i,j} + w_{p-1} I_{T-(p-1)}^{i,j}, ..., w_1 I_{T-1}^{i,j} \quad (6)$$

Where $w_p + w_{p-1} + ... + w_1 = 1$ and $w_1 > w_2 > ... > w_p$.

4. Calculation of optimal risk threshold: An optimal risk threshold is applied to the evaluation period. The threshold is obtained from the last data observations and execution of the methodology.

The optimal risk threshold is defined as the real number $\alpha_{last} \in R$ that maximizes the balanced accuracy (BACC). Balanced accuracy is defined as the average of the true positive and negative rates, $BACC = \frac{TPR+TNR}{2}$. The balanced accuracy is recommended when the data set is significatively imbalanced (Rocha-Salazar et al., 2021) as is commonly observed in financial crimes data sets. The following optimization problem is solved.

$$Max_{\{\alpha_{last}\}} \frac{TPR(\alpha_{last}) + TNR(\alpha_{last})}{2} \text{ for } \alpha_{last} \in R \quad (7)$$

5. Detection of suspicious cases: From the previous steps, it is observed that the suspicious activities detection falls on the monitoring of the connection intensities between two legal persons and their dynamics. Given the connection intensity between two legal persons "i", "j" in time

"T", it is first verified if said intensity is greater than the expected intensity (self-comparison). Then it is examined whether the same intensity (with implicit group-comparison) is greater than the optimal risk threshold α_{last}. If these two conditions are met, the connection is classified as suspicious.

If $I_T^{i,j} > \alpha_{last}$ *and* $I_T^{i,j} > I_{T_{expected}}^{i,j}$ *then classify the connection as suspicious*

The optimal risk threshold will define the normal and abnormal behaviour in the group. Connections whose intensities exceed the mentioned threshold will be considered abnormal concerning the group and normal otherwise. It will be a second group-comparison.

3.2.2. Methodology flow and computational algorithm

Financial institutions are subject to specific national and international regulations regarding the detection of financial crime. The treatment and analysis of transactions in search of suspicious activity have two stages: the objective and subjective stages. In the objective stage, the institution implements an automated system, an expert system that generates a set of suspicious cases without human intervention. In the subjective stage, the suspicious cases generated from the objective part are sent to the compliance department where they are thoroughly investigated by crime analysts. The analysts use their experience in past financial crimes, systems and applications to check the geolocation of the transactions. Moreover, they also analyze the people's financial statements, among other documents. Afterwards, the cases filtered by the subjective stage are sent to a risk and communication and control committee which decide what cases to send to the Financial Intelligence Unit (FIU). When the objective detection system has good accuracy, most of the resulting suspected cases successfully pass the subjective and filter stage of the committees. Once in the FIU, the cases are investigated again but now with criminal and legal resources. When a case is confirmed as a real crime by the FIU, the financial institution is notified to proceed with account blocking and the corresponding legal punishment. Notification of confirmed cases from the FIU to the financial institution is not done regularly since the investigation process varies from one transaction to another.

Taking the above insights, the flow of the proposed methodology in the objective component is shown in Fig. 1.

The raw data is extracted from the data warehouse, and it is processed in code through the following algorithm, as shown in Table 1:

The above algorithm is automated as an expert system and has been updated every month since June 2018. The compliance team sends the final report through an automated email sending process.

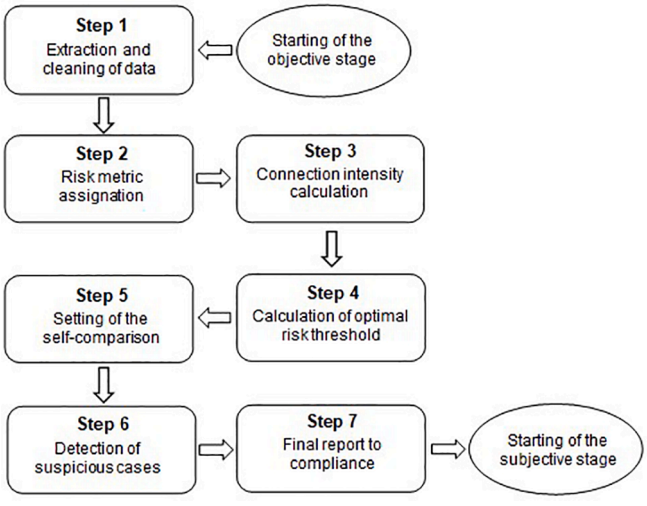

Fig. 1. Flow process. *Source*: Own elaboration.

Table 1
Computational algorithm.

1. Raw data extraction from Data Warehouse through SQL queries and cleaning
2. Identification of all the active legal persons in the evaluation period "T"
3. Creation of a database with the ClientID and the 14 risk attributes
4. Construction of a set with all the unique pairs of legal persons
5. Calculate n = number of unique pairs of legal persons in the institution
6. While $u<=n$ do:
   - 6.1 Take the pair of legal persons "i" and "j" of the observation u
   - 6.2 If the legal persons have at least one transaction in common
     - 6.2.1 Then define a connection in the social network
   - 6.3 Otherwise
     - 6.3.1 Leave aside the pair
7. Assign risk metrics by attribute to all the connected legal persons in the network
8. Sum the risk metrics of connected legal persons to have an aggregated risk vector
9. Compute the standard deviation of the aggregated risks by attribute from the whole network
10. Determine the connection intensity following the equation (4)
11. Compute the expected intensity for each connection in the evaluation period "T"
12. Take the optimal risk threshold from the last execution, α_{last}
13. Calculate s=number of unique pairs of legal persons in the social network
14. While $v<=s$ do:
    - 14.1 Take the connection intensity of legal persons "i" and "j" of the observation v
    - 14.2 If $I_T^{i,j} > \alpha_{last}$ and $I_T^{i,j} > I_{T_{expected}}^{i,j}$
      - 14.2.1 Then classify the connection as suspicious
    - 14.3 Otherwise
      - 14.3.1 Classify the connection as no suspicious
15. Make the final report and send it to compliance team for expert judgment investigations

Source: Compiled by the author. Clients are legal persons.

4. Data

Data from a financial institution in Mexico will be used to show the working of the proposed methodology. The variables extracted from the data warehouse are in line with the action mechanisms described in section 2.2, the experience of the compliance team in dealing with shell companies, and typologies observed in Secretariat of Finance and Public Credit (2016) and Force (2018) reports. The description is provided in Table 2:

Usually, a financial institution has thousands of legal entities that transact with each other and with legal entities of other institutions. This environment forms a complex network with millions of internal and

Table 2
Description of the variables used in this study.

Variable	Description
$\left\|\frac{out-in}{out}\right\|$	This variable is incorporated to track transactions related to the false invoice market
Economic activity	Legal person economic activity
PEP	Indicates whether the legal representative is politically exposed
Operations with the government	Indicates whether the legal person has operations with the government
Sense of address	Indicates whether the physical address coincides with the economic activity
Virtual offices	Indicates whether the legal person has virtual offices
Shareholders in common	Denotes whether the legal person has in common shareholders with other legal persons
Legal representatives in common	Denotes whether the legal person has in common legal representatives with the other connected legal person
Addresses in common	Indicates whether the legal person has a in common the address with the other connected legal person
Operability sense	Indicates whether the legal person transactions amounts coincide with its assets
Logic of financial relation	Refers whether the economic activity of linked legal persons makes sense
Deposited resources permanence	Average time between consecutive deposits and withdrawals
Shareholder's age	Average age of shareholders
Tenure	Time of relationship with the financial institution

Source: Own elaboration.

external connections. To show how the proposed methodology works, three random samples of 3,284, 2,550 and 3,148 connections of legal persons active in June 2019, September 2020, and November 2021 (evaluation periods) in the financial institution were taken, respectively. 52, 41 and 49 from the 3,284, 2,550, and 3,148 relationships are confirmed as shell companies' activities, respectively. As historical, social networks, those created monthly from June 2018 to May 2019, September 2019 to August 2020, and November 2020 to October 2021 were considered to set the expected/normal behaviour.

As mentioned, once the unique pairs of connected legal persons are defined for the evaluation period, the next step is the assignment of risk metrics for getting the intensity of the connections. The risk metrics for the institution in this study are defined as values from 0 to 100 without including 0. The elimination of zero is based on the logic that a legal entity will always have the latent risk of making transactions related to shell companies. Below we explain the criteria for the risk metrics assignment set by the compliance department and risk committee.

4.1. Measure $\left|\frac{out_t - in_t}{out_t}\right|$

The risk assignation for this measure in the month "t" is as shown in Table 3:

When a shell company is made with the goal of trading fake invoices, a well-defined pattern is observed according to Barajas et al. (2011) and Cruz-Pérez (2020). The shell company offers a fictitious product "g" at an "*out*" price to another company (recipient) that wishes to deduct the tax rate "δ". The receiving company pays "*out*" and almost immediately receives back the amount "*in*" less than "*out*" from the shell company by electronic transfer. The difference $out - in$ represents the profit of the shell company and $\delta \cdot out$ the amount deducted by the receiving company before the tax authority. The benefit for the recipient company is obtained when $\left|\frac{out_t - in_t}{out_t}\right| < \delta$. Experience in Mexico shows that this proportion is commonly<10% and between 10% and 16% in a few cases. 16% is the value-added tax in Mexico. For this reason, the metric $\left|\frac{out_t - in_t}{out_t}\right|$ is created and it is assigned a higher risk in values<0.16 and greater than 0. The absolute value is applied to contemplate that any of the two connected legal entities can be a buyer or a seller of fictitious invoices.

4.2. Economic activity

The institution has over 1000 types of economic activities. These are classified into three levels of risk according to their relationship with the action mechanisms of shell companies. The high risk is assigned the metric 100, the medium 60 and the low 20. In this way, legal entities with economic activities such as real estate investments and charity will have a metric of 100, and those with agricultural activities will have a metric of 20, as an example.

4.3. Politically exposed people, operations with the government, address sense and virtual offices

These are binary variables classified as high risk if the attribute is present and low otherwise. If the legal representative of the legal entity is politically exposed, it is assigned a metric 100 and 3.33 otherwise. If the legal entities have at least one operation with the government in the month of analysis, it is assigned the value of 80 for high risk and 20 for the low one. When the economic activity of the legal entity does not coincide with what is observed in the physical address, it is assigned a risk value of 90 and 15 otherwise. An example of non-coincidence is observed when the legal entity declares that his economic activity is the sale of jewellery, but in his physical address, it turns out to be a common home. The presence of virtual offices makes it more challenging to verify the real existence of a company's operations. It is one of the mechanisms used by shell companies to hide their identity. For this reason, operation through virtual offices assigns a value of 100 for high risk and 10 for low.

Table 3
Assigned metrics.

Value	Risk Metric
$\left\|\frac{out_t - in_t}{out_t}\right\|$<=0.1 - {0}	100
0.1<$\left\|\frac{out_t - in_t}{out_t}\right\|$ < 0.16	80
Other	10

Source: Own elaboration.

4.4. Economic shareholders, legal representatives, and addresses in common

For these variables, two levels of risk are defined, low and high. If the connected legal entities have legal representatives in common, a value of 100 is assigned for high risk and 10 for low risk. In the same way for addresseses in common, the high risk is assigned metric 70 and 10 for the low one. If the legal entities have shareholders in common with other legal entities even though they are not connected, a value of 85 is assigned for high risk and 15 for low risk.

4.5. Operability sense

The return on assets (ROA) is a financial ratio used to measure the ability of the company to generate income with its assets under management. It is calculated for a certain period "t", for example, monthly, and is mathematically expressed as $ROA_t = \frac{Net\ \ income_t}{Total\ \ assets_t}$. Banks usually use this ratio to measure the profitability of a company when granting it a loan. Values of this ratio between 0.05 and 0.5 are considered acceptable and greater than 0.5 more than acceptable. Shell companies by their part tend to have much greater returns than other similar licit entities due to the lack of systematic risks and assets (Floros & Sapp, 2011).

To determine if the operation of a legal entity coincides with its managed assets, the RT_t reason is defined for the period "t". This measure expresses the proportion that the transactions made by the legal entity represent of the total assets, mathematically it is calculated as:

$$RT_t = \frac{Sum\ \ of\ \ transactions\ \ amounts_t}{Total\ \ assets_t} \tag{8}$$

It is assumed that the sum of transaction amounts made in period "t" is positively correlated with the income received in the same period "t". Under this pattern, it is decided to make a classification into three risk levels for the RT_t measure. It is assigned a value of 100 for high risk when $RT_t >= 1$, 55 for medium risk when $0.5 <= RT_t < 1$ and 10 for low risk when $0 <= RT_t < 0.5$.

4.6. Logic of financial relation

This variable has three levels of risk created based on the sense of the business relationship between two legal persons. For example, a legal person dedicated to producing livestock feed will have a close and meaningful relationship with a legal person dedicated to the breeder and sale of livestock. A legal person devoted to the specific sale of laptops and cell phones will have an average relationship with a legal person dedicated to producing household electrical appliances. The relationship between a jewellery store makes little sense with a legal person involved in footwear production. For a sense of commercial relationship, a high-risk value of 90 is assigned, 50 for medium sense and 10 for low sense.

4.7. Permanence of deposited resources

As described in section 2, two of the stages of money laundering in financial systems are the introduction of resources (placement) and their distribution in other accounts (layering). A suspicious pattern observed in money laundering and fraud cases is that the deposited resources have little permanence in the initial account. The criminal tries to move the resources to other accounts as soon as possible to blur their origin. Under this behaviour, the following risk metrics are assigned according to Table 4:

4.8. Shareholders' age

Having young shareholders, including minors age, are common patterns observed in the action mechanisms of shell companies. It is intended to divert attention from the primary beneficiary. Since a legal person can have more than one shareholder, their average age is calculated, and the risk metric is assigned according to Table 5.

4.9. Tenure

The short lifespan of shell companies is an important feature and why they are sometimes called "ghost companies". They appear to serve as a vehicle to commit various crimes and then disappear in a short time before being discovered. Based on this mechanism of action, the risk metrics assigned to the different tenure levels are shown in Table 6.

4.10. Network and intensities creation

In a particular evaluation month, the raw data of active customers is extracted from the data warehouse with all their attributes in the form of columns. Subsequently, a risk value is assigned according to the value of the attributes. Table 7 shows the attributes as extracted and risk metrics assigned for two connected legal persons in June 2019 (two legal persons with transactions in at least one direction).

If the legal entity has virtual offices, "YES" is assigned, otherwise "NO". If the economic relationship between two legal entities makes sense, "YES" is given, otherwise "NO". If companies have operations with the government, "YES" is assigned, otherwise "NO". If the financial operation of the entities makes sense with their assets, "YES" is given, otherwise "NO". If two legal entities have addresseses, legal representatives, or shareholders in common, "YES" is assigned, otherwise "NO". If the physical address of the legal entity makes sense with its economic activity, "YES" is set, otherwise "NO". Fig. 2 shows how the connection of the two legal persons "C8270" and "C9676" are represented in the social network.

The connection intensity is obtained using equation (4), whose weights are the standard deviations of the attributes in the data set.

$$I^{C8270,C9676}_{June\ 2019} = \frac{64.36(100+100)+39.99(100+40)+\ldots+54.57(80+100)}{64.36+39.99+\ldots+54.57} = 164.08 \tag{9}$$

Regarding the 12-month history for this connection, Table 8 shows the intensities recorded.

Table 4
Assigned metrics.

Average permanence of deposited resources	Risk metric
One day	100
One week	80
Two weeks	60
One month	40
More than one month	20

Source: Own elaboration.

Table 5
Assigned metrics for shareholders' age.

Shareholder average age	Risk metric
No identified	100
Average age < 18	100
18 <= Average age < 65	33.33333333
Average age >=65	66.66666667

Source: Own elaboration.

Table 6
Assigned metrics for tenure.

Tenure	Risk metric
Tenure < 1 years	100
1 year <=Tenure < 3 years	75
3 years <=Tenure < 5 years	50
Tenure >=5 years	25

Source: Own elaboration.

Table 7
Raw data.

	Attribute Values		Risk Metric	
Client ID	C8270	C9676		
Virtual offices	YES	YES	100	100
Resource permanence	One day	One month	100	40
Financial relationship	NO	NO	90	90
Tenure	Tenure < 1 years	3 years <=Tenure < 5 years	100	50
Operations with government	YES	YES	80	80
Operability sense	NO	NO	100	100
Economic activity	LOW	HIGH	20	100
PEP	YES	YES	100	100
Addresses in common	YES	YES	70	70
Legal representatives in common	YES	YES	100	100
Average shareholders age	18 <= Average age < 65	18 <= Average age < 65	33.33	33.33
Shareholders in common	YES	YES	85	85
Address sense	NO	YES	90	15
False invoice criterium	MEDIUM	HIGH	80	100

Source: Own elaboration.

Table 8 shows the expected connection intensity for the given couple of nodes taking as weights the increasing probabilities. It is observed that the connection intensity of the evaluation period (164.08) is greater than the expected connection intensity (150.5811). If, in addition to this, the connection intensity in the evaluation period is greater than the optimal risk threshold, the connection will be classified as suspicious.

5. Results and discussion

Currently the methodology is implemented in a financial institution and executed monthly automatically. To show the results obtained from its application, 3 different evaluation periods were considered, June 2019, September 2020, and November 2021. Fig. 3 shows the social networks resulting from the random samples taken.

If we zoom one of them, we can observe the connection intensities between nodes, the number in the middle of the link. See Fig. 4.

From Fig. 4 it can be observed that because the sum of the weights in the intensity function is equal to 1 and the individual risk metrics are in the range (0,100], the value of the connection intensity fluctuates in the range (0, 200]. At first glance, it seems tempting to think that suspicious connections would be in the densest part of the network. In those legal entities that make a greater number of transactions with other entities in

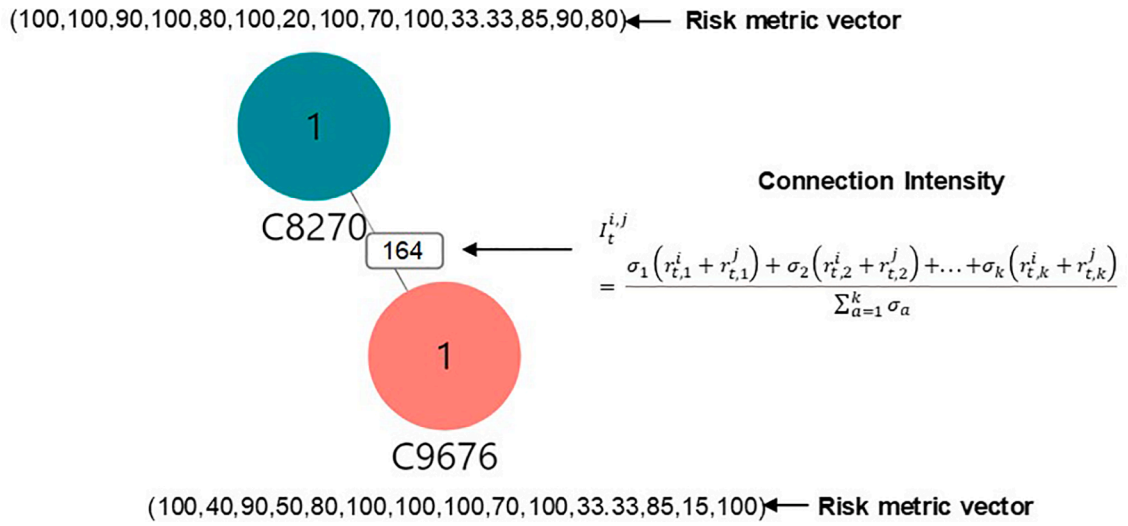

Fig. 2. Nodes connection. *Source*: Own elaboration.

Table 8
Historical social networks.

Month	Connection Intensity	Group Comparison Probabilities (Weights)
June 2018	150.2421339	0.0628
July 2018	145.549936	0.0659
August 2018	149.8475475	0.0692
September 2018	152.9631814	0.0726
October 2018	141.2373594	0.0763
November 2018	155.8850222	0.0801
December 2018	156.3391216	0.0841
January 2019	149.5647064	0.0883
February 2019	147.909981	0.0927
March 2019	141.7581894	0.0974
April 2019	163.0857826	0.1022
May 2019	150.1494249	0.1084
Expected Connection Intensity	**150.5811**	

Source: Own elaboration.

a certain period. But as is explained in sections 3.1 and 3.2, this does not always suggest suspicious activity. For the financial institution of this article, high-density areas of the network correspond to transactions between legal persons belonging to the same geographical location and similar economic activities rather than suspicious behaviour. Therefore, focusing on connection intensities rather than high-density areas is more relevant.

For the self-comparison, the compliance committee decides to give an initial weight of 0.0628 for the intensities of the oldest network with successive increases of 5% for the intensities of more recent networks. The initial weight is the initial term of a geometric progression with ratio 1.05 (so that the terms grow 5%) and whose sum of 12 terms is 1 (12 terms because we have 12 months of history). Part of the dynamic structure of the historical networks is shown in Fig. 5.

Once the last optimal risk threshold and expected intensities are determined, the rule defined in section 3.2 is implemented.

If $I_T^{i,j} > \alpha_{last}$ *and* $I_T^{i,j} > I_{T_{expected}}^{i,j}$ *then classify the connection as suspicious*

In other words, if the connection intensity between the legal entities "i", "j" is greater than a predetermined risk threshold and in turn greater than the expected intensity, the connection is classified as suspicious, and an alert is generated. Due to the connection intensity takes values in the range (0,200], the predetermined threshold α_{last} can vary in the same interval. Historically, the last optimal risk threshold α_{last} for the company has fluctuated from 130 to 140 obtained in the different evaluation months. It is important to mention that this is not a typical supervised or unsupervised machine learning methodology where training and test sets are usually defined. The proposed method takes the last optimal risk threshold available from the last evaluation and incorporates it into dynamic social networks to classify future connections as "suspicious" or "not suspicious". This optimal threshold is not obtained from month to month regularly since it depends on the existence of confirmed real cases. In some months, the number of confirmed cases can be zero, 1 or 2, not enough for a recalibration. The availability of confirmed cases depends on the joint investigation times of the compliance, risk and intelligence unit areas that do not generate results on a regular basis. Despite this, experience has shown excellent results in the evaluation period, even when an optimal threshold obtained up to one year ago is used. The reason is that from the 14 variables proposed in Table 2, only permanence of deposited resources, operations with the government, operability sense and $\left|\frac{out_t - in_t}{out_t}\right|$ change significantly from one month to another, while the rest of the variables suffer minimal variations.

Fig. 6 shows the different balanced accuracies, and thresholds for the three evaluation periods tested. The optimal risk thresholds are 137 and 138, achieving a balanced accuracy above 0.90. This shows the existence of an optimal threshold for which the proposed methodology performs very well.

Table 9 shows the balanced accuracy from the application of the methodology using the 137 and 138 as the values of α_{last}. The results of the proposed methodology were compared with those ones of the previous system. The financial institution implemented a rule-based system with the problem of low accuracy and high false positive rates. The rules are made up of a set of conditions that portray a suspicious profile of transactions. Conditions are joined by logical operators such as "AND" or "OR". For example, a suspicious transaction profile can be defined if the customer is a politically exposed person (PEP), and the transaction amount exceeds 10,000 USD. It may be noted that this suspicious profile has 2 conditions that must be fulfilled at the same time. Condition (1) is "The client is PEP", condition (2) is "Transaction amount exceeds 10,000 USD", and the need for both conditions to be met at the same time is resolved by joining them with "AND". Usually a rule-based system has tens or hundreds of rules for various risk profiles. The comparison is shown below.

It is observed that the proposed methodology has significantly better detection accuracy than the previous rule system in the three evaluation periods. The accuracy is stable over time in the first method (proposed),

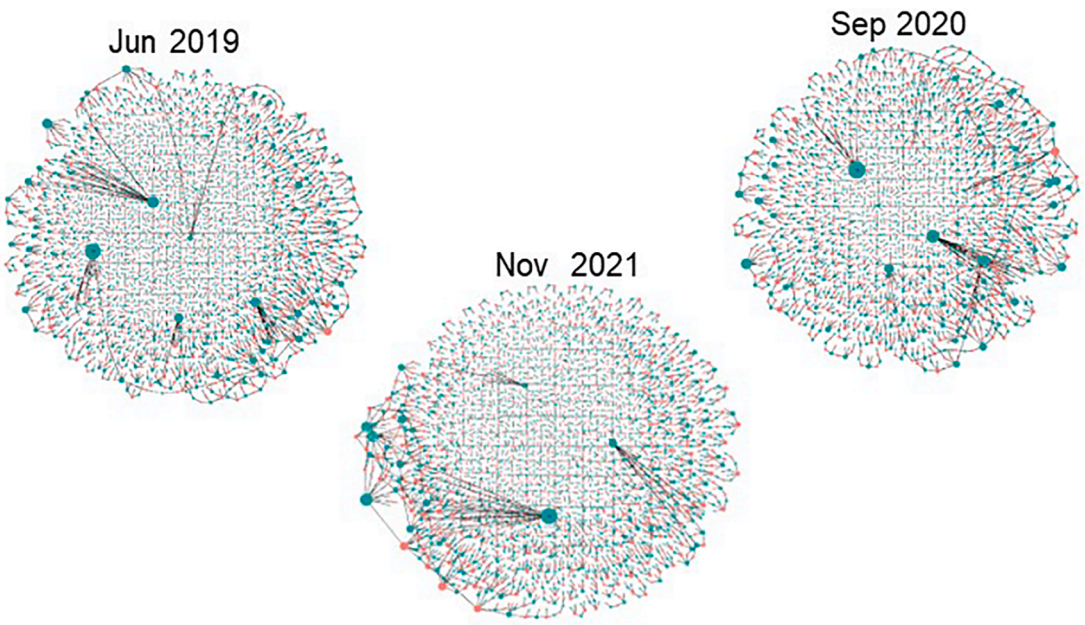

Fig. 3. Description of social networks. *Source*: Own elaboration.

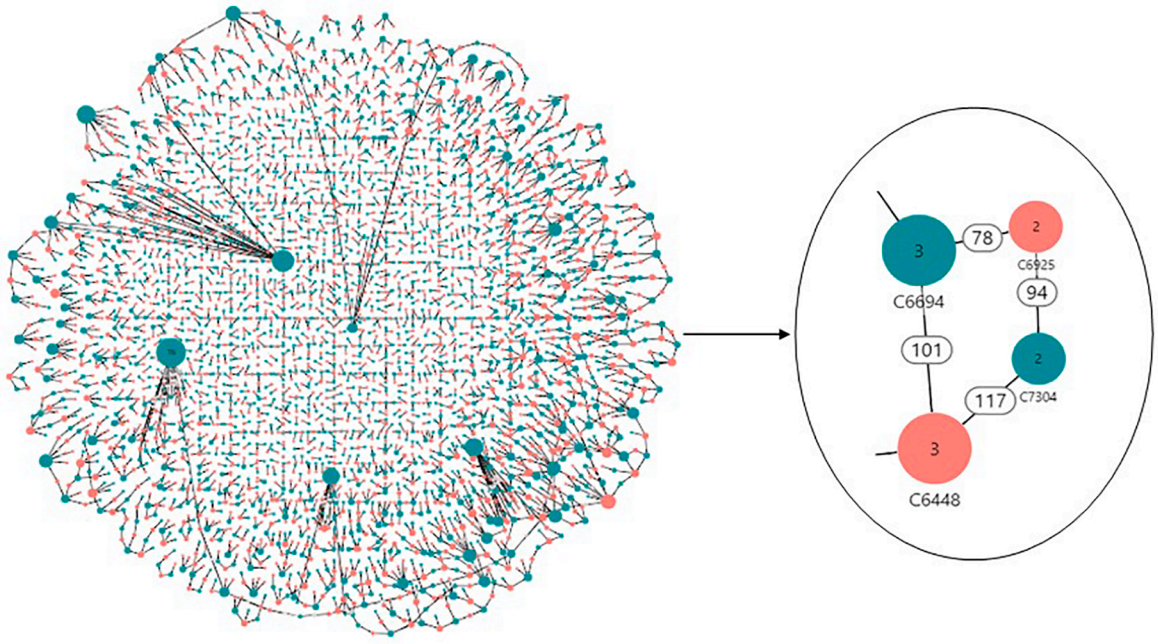

Fig. 4. Zoom description of connection intensities. *Source*: Own elaboration.

while in the second one (rule system) is more fluctuating. In fact, a decrease in the accuracy is noted for the rule system in September 2020 that the pandemic emergence might cause. The proposed model remained stable in the same period, even with an increase in the accuracy. Stability is a characteristic that is sought in every detection model that avoids recalibrations and profound changes in its design in the short term. Rule models tend to be unstable, requiring constant recalibration of their conditions, thresholds, and logic. A disadvantage that implies more time invested by the development team and more extra costs. Turning to specific metrics, the true positive rate is also notoriously higher in the proposed methodology than in the rules system. It is also more stable in the three evaluation periods. Although the false positive rate does not look high in both models, the rules methodology doubles the rate of the proposed methodology in September 2020 and November 2021. This difference becomes important when the number of daily transactions is counted in the millions. The cases classified as suspicious are investigated by the risk and compliance committees involving human resources, time, and monetary costs. If the false-positive rate is as low as possible, the mentioned demands are also reduced. What is observed as a relevant problem is the false negative rate, which is markedly great in the rules methodology in the three evaluation periods. A high rate of false negatives implies many suspected cases not successfully detected.

The high level of accuracy of the proposed methodology shows that the detection of shell companies in the financial systems strongly depends on the interaction of various attributes in the flow of transactions.

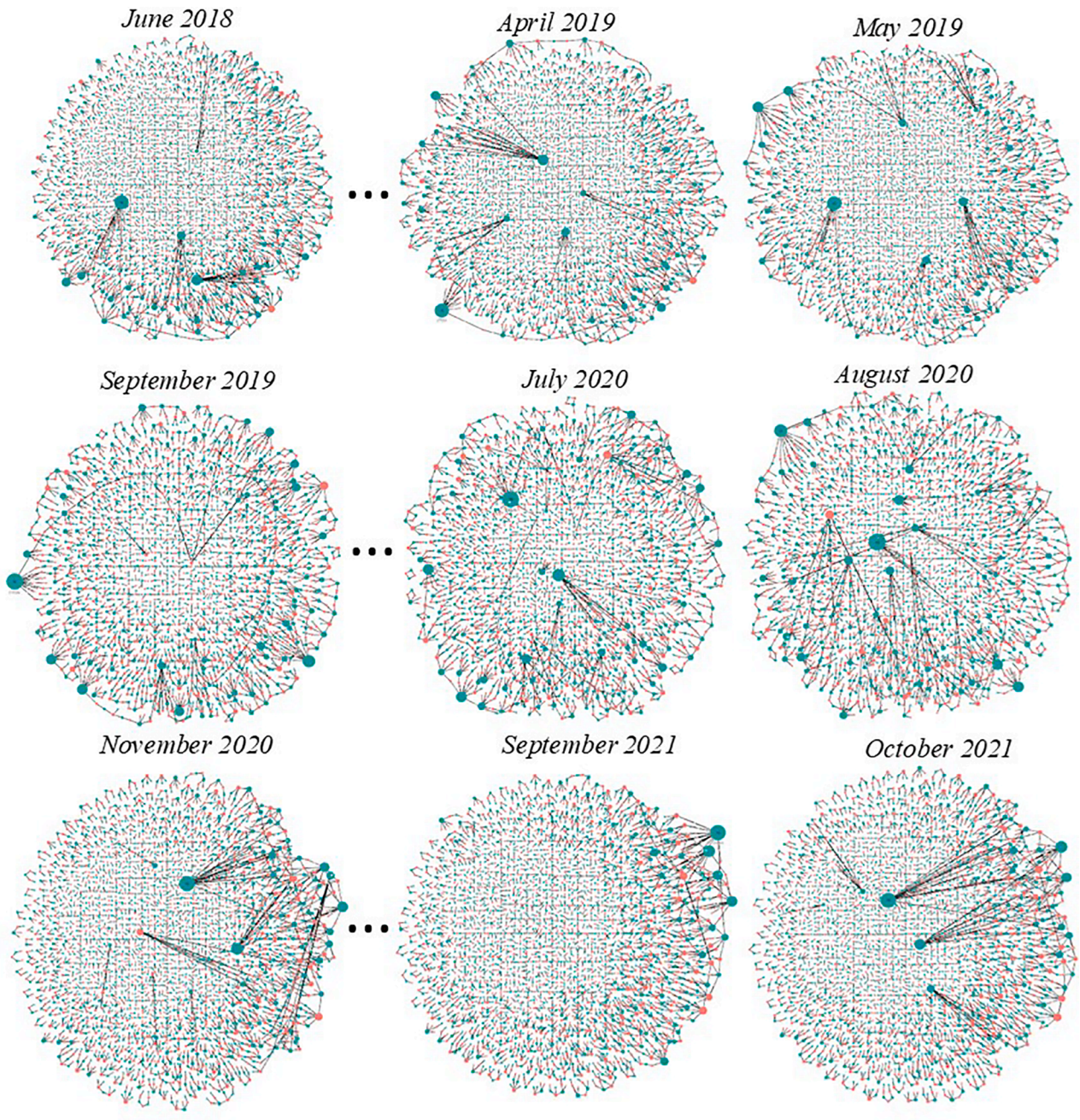

Fig. 5. Historical social networks. *Source*: own elaboration.

Centrality metrics as those implemented by Joaristi et al. (2019) and Tiwari et al. (2021) can be biased by flows between companies with related economic activities (economic relations that make sense) and financial operations in the same geographic areas. Mechanism and techniques of shell companies' action as those reported by FATF are also of great importance. Although studies as Pawde et al. (2018) and Luna et al. (2018) have considered the industrial sector, number of employees and revenues, in simulated data, the reality in financial systems makes necessary to incorporate more mechanisms present in the interaction between legal entities such as the nature of business relations, addresseses in common, virtual offices, etc. The same applies when metrics obtained from financial statements are considered as the main criteria of detection, as in Aggarwal and Dharni (2020). There are many reasons why a company's transactionality does not match its revenues or recorded assets. In the financial system it is common to see legal entities with peak sales periods (with atypical revenue increase) maintaining the same level of assets without necessarily being shell companies. The latter originated by the sudden launch of temporary campaigns and promotions or beneficial macroeconomic conditions. Also, it is observed legal entities with revenues that match their assets, stable transactionality and healthy financial ratios, but a deeper look reveals that they are in a stable market of fake invoices through a virtual office with other companies with the same legal representatives and shareholders.

The detection of shell companies in financial institutions must be a task with methodologies adapted to their particular mechanisms of action. Its detection should not be considered as implicit in methodologies to detect money laundering, corruption, fraud or other financial crimes. This would vanish the chances of successful detections.

6. Conclusions

This study proposed an innovative methodology that incorporates

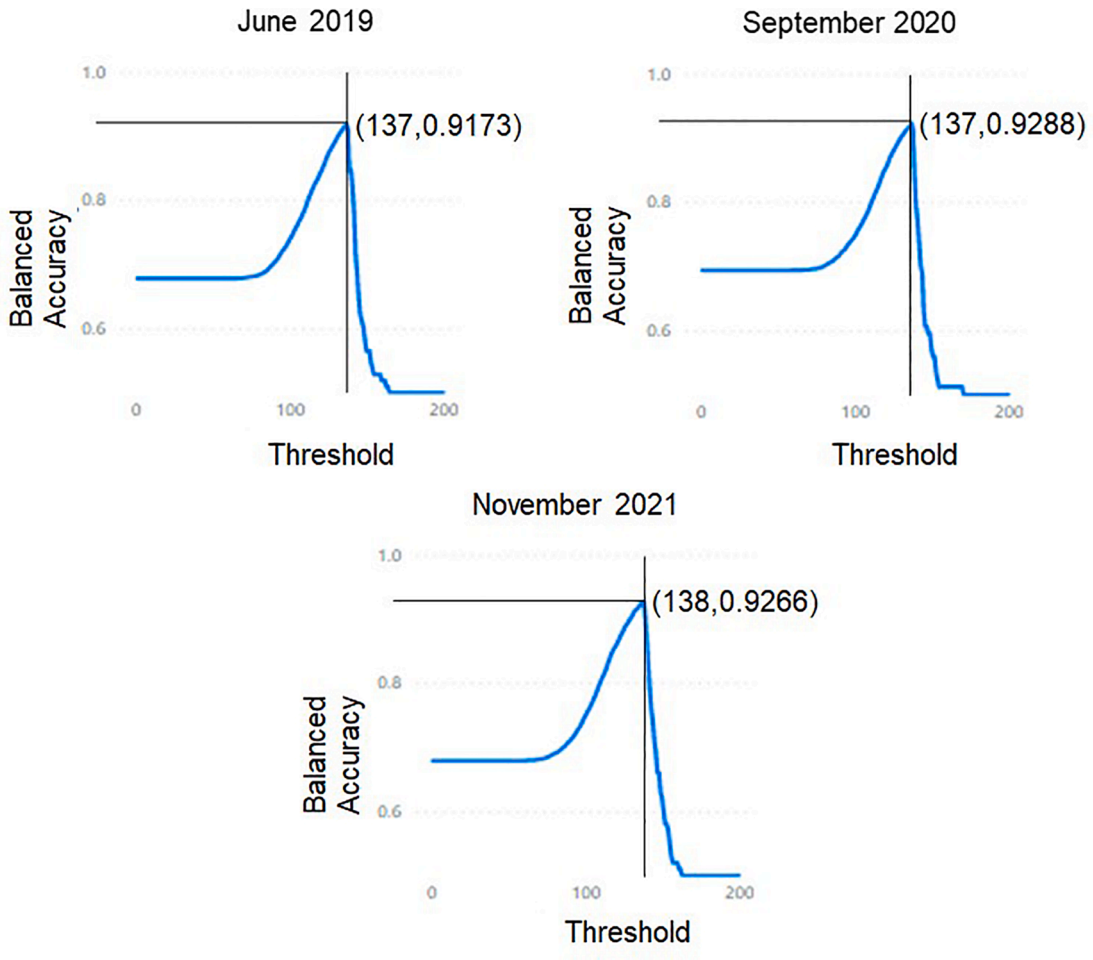

Fig. 6. Balanced accuracy vs threshold. *Source*: own elaboration.

Table 9
Methodologies comparison.

June 2019		
Measure	**Proposed**	**Rule System**
True positive rate	0.8654	0.2692
False positive rate	0.0306	0.0294
True negative rate	0.9694	0.9706
False negative rate	0.1346	0.7308
BACC	0.9174	0.6199
September 2020		
Measure	**Proposed**	**Rule System**
True positive rate	0.8780	0.1707
False positive rate	0.0323	0.0658
True negative rate	0.9677	0.9342
False negative rate	0.1220	0.8293
BACC	0.9229	0.5525
November 2021		
Measure	**Proposed**	**Rule System**
True positive rate	0.8776	0.2245
False positive rate	0.0242	0.0400
True negative rate	0.9758	0.9600
False negative rate	0.1224	0.7755
BACC	0.9267	0.5922

Source: Own elaboration.

group and self-comparisons into dynamic social networks for the detection of shell companies. The existence of an optimal risk threshold that maximizes the balanced accuracy prediction is shown. Also, with the mentioned threshold, it is possible to obtain a low acceptable rate of false positives that contribute to reducing time, human resources, and financial costs in suspicious cases investigations of shell companies.

Currently the technique is implemented in an important Mexican financial company with positive results. Inspired by this, any institution is motivated to make full or partial use of the proposal presented according to its need. The mass application of the proposed methodology by financial institutions would allow the timely identification of shell companies and the implementation of sanctions by the financial intelligence units. This would give the governments of the countries greater control over shell companies' activities and therefore, a reduction in their main crimes of tax avoidance and money laundering cases.

However, this article is not free of limitations. In the implementation, it is also recommended to consider the fact of not regularly owning with confirmed cases of shell companies to obtain the optimal risk threshold. This can cause a particular bias in predicting cases when the period between the last optimal threshold obtaining, and the evaluation period is very long (for example, more than one year). Another limitation is not considering connections with clients in other financial institutions. From the latter, future investigation lines will be focused on modelling suspicious internal connections and connections between an internal legal person and an external one belonging to another financial institution.

CRediT authorship contribution statement

José-de-Jesús Rocha-Salazar: Writing – original draft, Formal analysis, Conceptualization, Methodology, Software. **María-Jesús Segovia-Vargas:** Project administration, Writing – review & editing, Validation, Funding acquisition. **María-del-Mar Camacho-Miñano:**

Visualization, Writing – review & editing, Validation, Resources.

Declaration of Competing Interest

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

Acknowledgments

This research was supported by Spanish Ministry of Science and Innovation research project, with reference PID2020-115700RB-I00.

Declaration Statement

This manuscript is the authors' original work and has not been published nor has it been submitted simultaneously elsewhere. All authors have checked the manuscript and have agreed to the submission.

References

Aggarwal, V., & Dharni, K. (2020). Deshelling the shell companies using benford's law: An emerging market study. *The Journal for Decision Makers, 45*(3), 160–169. https://doi.org/10.1177/0256090920979695

Allred, B. B., Findley, M. G., Nielson, D., & Sharman, J. C. (2017). Anonymous shell companies: A global audit study and field experiment in 176 countries. *Journal of International Business Studies, 48*, 596–619. https://www.jstor.org/stable/45149377.

Avendaño, F., & Chávez, I. (2019). *El arte de la simulación: casos emblemáticos de corrupción en México.* [The art of simulation: emblematic cases of corruption in Mexico]. Instituto Mexicano para la Competitividad A.C. http://hdl.handle.net/11445/3936.

Barajas, S., Campos, R., Sobarzo, H., & Zamudio, A. (2011). *Evasión fiscal derivada de los distintos esquemas de facturación* [Tax evasion derived from the different invoicing schemes] Center for Economic Studies. *Mexican College.* http://omawww.sat.gob.mx/cifras_sat/Documents/2010_eva_fis_der_dis_esque_fac.pdf.

Bright, D., Brewer, R., & Morselli, C. (2021). Using social network analysis to study crime: Navigating the challenges of criminal justice records. *Social Networks, 66*, 50–64. https://doi.org/10.1016/j.socnet.2021.01.006

Cooley, A., Heathershaw, J., & Sharman, J. C. (2018). The rise of kleptocracy: Laundering cash, whitewashing reputations. *Journal of Democracy, 29*(1), 39–53. https://muse.jhu.edu/article/683634.

Cruz-Pérez, B. L. (2020). *Mercado de facturas apócrifas en México: Un análisis teórico de las operaciones simuladas como medio de evasión fiscal.* [The market for apocryphal invoices in Mexico: A theoretical analysis of simulated transactions as a means of tax evasion]. *General Coordination of Postgraduate Studies, UNAM, Thesis and repository harvest of the General Directorate of Libraries and Digital Information Services*. https://repositorio.unam.mx/contenidos/ensayo-que-lleva-por-titulo-mercado-de-facturas-apocrifas-en-mexico-un-analisis-teorico-de-las-operaciones-simuladas-c-3543951?c=4XQ9ab&d=false&q=*:*&i=1&v=1&t=search_0&as=0.

Das, K., Samanta, S., & Pal, M. (2018). Study on centrality measures in social networks: A survey. *Social Network Analysis and Mining, 8*, 13. https://doi.org/10.1007/s13278-018-0493-2

Diestel, R. (1990). *Graph decompositions: A study in infinite graph theory* (1st ed.). Clarendon Press.

FFIEC. (2009, July). The detection and deterrence of mortgage fraud against financial institutions: a white paper. Fraud Investigations Symposium. https://www.ffiec.gov/exam/Mtg_Fraud_wp_Feb2010.pdf.

Force. (2014). Transparency and beneficial ownership. Financial Action Task Force. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/guidance-transparency-beneficial-ownership.pdf. Accessed May 19, 2022.

Force. (2018). Concealment of beneficial ownership. Financial Action Task Force. Retrieved from https://www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html. Accessed May 19, 2022.

Floros, I. V., & Sapp, T. R. A. (2011). Shell games: on the value of shell companies. Journal of Corporate Finance, 17(2011), 850–867. http://www.sciencedirect.com/science/article/pii/S0929119911000198.

Fronzetti Colladon, F., & Remondi, E. (2016). Using social network analysis to prevent money laundering. *Expert Systems with Applications, 67*, 49–58. https://doi.org/10.1016/j.eswa.2016.09.029

Jancsics, D. (2017). Offshoring at home? domestic use of shell companies for corruption. *Public Integrity, 19*(1), 4–21. https://doi.org/10.1080/10999922.2016.1200412

Jancsics, D. (2018). Shell companies and government corruption. *Global Encyclopedia of Public Administration, Public Policy, and Governance*. Springer. https://doi.org/10.1007/978-3-319-31816-5_3566-1.

Joaristi, M., Serra, E., & Spezzano, F. (2019). Detecting suspicious entities in offshore leaks networks. *Social Network Analysis and Mining, 9*(1), 1–15. https://doi.org/10.1007/s13278-019-0607-5

Larik, A. S., & Haider, S. (2011). Clustering based anomalous transaction reporting. *Procedia Computer Science, 3*, 606–610. https://doi.org/10.1016/j.procs.2010.12.101

Luna, D. K., Palshikar, G. K., Apte, M., & Bhattacharya, A. (2018). Finding shell company accounts using anomaly detection. In *In Proceedings of the ACM India Joint International Conference on Data Science and Management of Data. January* (pp. 167–174). https://doi.org/10.1145/3152494.3152519

Morselli, C., & Petit, P. (2007). Law-enforcement disruption of a drug importation network. *Global Crime, 8*(2), 109–130. https://doi.org/10.1080/17440570701362208

Morselli, C. (2009). Inside criminal networks (1st ed.). Springer. https://link.springer.com/book/10.1007/978-0-387-09526-4.

Nielson, D. & Sharman, J. (2022). *Signatures for sale: How nominee services for shell companies are abused to conceal beneficial owners*. Stolen Asset Recovery Initiative. World Bank Group. Retrieved from https://openknowledge.worldbank.org/handle/10986/37335?locale-attribute=es. Accessed May 12, 2022.

Pacini, C., Hopwood, W., Young, G., & Crain, J. (2018). Thace role of shell entities in fraud and other financial crimes. *Managerial Auditing Journal, 34*(3), 247–267. https://doi.org/10.1108/MAJ-01-2018-1768

Pawde, A., Apte, M., Palshikar, G. K., & Attar, V. (2018). Synthesizing data for collusion-based malpractice of shell companies in money laundering. *IEEE*. https://ieeexplore.ieee.org/document/9058145.

Quintana-Adriano, E.A. (2015). Natural persons, juridical persons, and legal personhood. *Mexican Law Review*, 8(1), 101-118. ISSN 2448-5306.

Rocha-Salazar, J. J., Segovia-Vargas, M. J., & Camacho-Miñano, M. M. (2021). Money laundering and terrorism financing detection using neural networks and an abnormality indicator. *Expert Systems with Applications, 169*(1), Article 114470. https://doi.org/10.1016/j.eswa.2020.114470

Ruehsen, M., & Spector, L. (2015). Follow the proliferation money. *Bulletin of the Atomic Scientists, 71*(5), 51–58. https://doi.org/10.1177/0096340215590798

Schuknecht, L., & Siegerink, V. (2021). *The political economy of the international tax transparency agenda in the G20/OECD context*. CESifo Working Papers ISSN 2364-1428. CESifo Working Papers ISSN 2364-1428.

Secretariat of Finance and Public Credit (2016). First national risk assessment. https://www.pld.hacienda.gob.mx/work/models/PLD/documentos/enr.pdf.

Secretariat of Finance and Public Credit (2019). LXIV legislature of the honorable congress of the union. https://infosen.senado.gob.mx/sgsp/gaceta/64/2/2019-09-05-1/assets/documentos/DIC_HACIENDA_COMPETIR_IGUALDAD.pdf.

Singh, D. (2010). Incorporating with fraudulent intentions. A study of various differentiating attributes of shell companies in India. *Journal of Financial Crime, 17*(4), 459–484. https://doi.org/10.1108/13590791011082805

Singh, K., & Best, P. (2019). Anti-money laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems, 34*(100418). https://doi.org/10.1016/j.accinf.2019.06.001

Tabassum, S., Pereira, F. S. F., Fernandes, S., & Gama, J. (2018). Social network analysis: An overview. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 8*(5). https://doi.org/10.1002/widm.1256

Tang, L., Barbier, G., Liu, H., & Zhang, J. (2010). A social network analysis approach to detecting suspicious online financial activities. *Advances in Social Computing, Lecture Notes in Computer Science, 6007*. https://doi.org/10.1007/978-3-642-12079-4_49

The Guardian (2017a). *Revealed: Justin Trudeau's close adviser helped move huge sums offshore*. Retrieved from https://www.theguardian.com/news/2017/nov/05/justin-trudeau-adviser-stephen-bronfman-offshore-paradise-papers. Accessed May 12, 2022.

The Guardian (2017b). *Tory ex-minister who defended tax avoidance has Bahamas trust fund*. Retrieved from https://www.theguardian.com/news/2017/nov/07/tory-ex-minister-james-sassoon-bahamas-trust-fund. Accessed May 12, 2022.

Tiwari, M., Gepp, A., & Kumar, K. (2020). A review of money laundering literature: The state of research in key areas. *Pacific Accounting Review, 32*(2), 271–303. https://doi.org/10.1108/PAR-06-2019-0065

Tiwari, M., Gepp, A., & Kumar, K. (2021). July). *Shell companies: Using a hybrid technique to detect illicit activities. Poster session presented at 2021 Accounting and Finance Association of Australia and New Zealand (AFAANZ) Virtual Conference*.

Vail, N. (2018). Cracking shells: The Panama papers & looking to the European Union's anti-money laundering directive as a framework for implementing a multilateral agreement to combat the harmful effects of shell companies. *5 Tex. A&M L, 5*(1), 133–153. https://doi.org/10.37419/LR.V5.I1.4