UNIVERSITÉ DE MONTRÉAL

BOILER ROOMS – STRUCTURE, EMPLACEMENTS ET *MODUS OPERANDI*

PAR CLARISSE LAINÉ

ET EMANUELLE MARY

FACULTÉ DES ARTS ET DES SCIENCES ÉCOLE DE CRIMINOLOGIE

TRAVAIL PRÉSENTÉ À MASARAH PAQUET-CLOUSTON

DANS LE CADRE DU COURS CRI6228A-A22

CRIMINALITÉS ÉCONOMIQUES

DÉCEMBRE 2022

Résumé

Apparues dans les années 1920 aux États-Unis, les *boiler rooms* se sont définies comme des centres d'appels depuis lesquels s'organisent des fraudes à l'investissement. De nombreuses évolutions ont impactées les *boiler rooms* dans leurs emplacements et leurs structures. Les fraudeurs utilisent toutes sortent de méthodes, techniques, psychologiques ou économiques pour arriver à leurs fins. Ils useront de ces méthodes pour obtenir le maximum d'argent de leurs victimes, dès le premier contact même lorsque la victime a montré sa volonté de se retirer. Les *boiler rooms* s'insèrent dans des organisations criminelles qui emploient plusieurs centres d'appels dans le but de réaliser des fraudes. Une véritable hiérarchie se construit au sein de celles-ci et de nombreux collaborateurs sont impliqués dans les actions criminelles. L'évolution des emplacements des *boiler rooms* à travers le monde est guidé par les répressions policières et par les changements de législations des pays où ils s'implantent et où sont situées leurs victimes. Les groupes de fraudeurs disposent de différents types de locaux. Ceux-ci ont évolué au cours du temps, en commençant à l'origine par de petites pièces dans les sous-sols d'immeubles américains. Actuellement, des chambres d'hôtel ou des bureaux mobiles peuvent abriter des fraudes de ce type.

Table des matières

Introduction

La fraude liée à la vente d'actions est le type de fraude causant le plus de pertes monétaires, notamment au Canada où elle cause la perte de montants s'élevant à plus de 164 millions de dollars canadiens, sur environ 3442 signalements en 2021 (Centre antifraude du Canada, 2021). Ce phénomène est loin de ne s'illustrer qu'au Canada. Un rapport d'AMF France montre que « 61% des Français ont été exposés à une proposition de placement alternatif » et 1% de la populations (ce qui correspond à plus de 650 000 personnes) ont potentiellement été victimes d'arnaques à l'investissement (AMF, 2021). En Australie, il a été estimé qu'entre 2007 et 2012, plus de 113 millions de dollars australiens avaient été perdus dans le cadre de la fraude à l'investissement (Drew & Cross, 2013).

La fraude à l'investissement peut s'opérer de diverses manières. Ce travail va se consacrer à un type de fraude à l'investissement apparu au XX^{ème} siècle et ayant été largement médiatisé, notamment par le biais de films à succès comme « *Boiler Room* » (2000) et « *The Wolf of Wall Street* » (2013), inspirés par le cas du fraudeur Jordan Belfort. Il s'agit de la fraude de type *boiler room*.

C'est un type de fraude téléphonique qui se distingue du télémarketing par son caractère illégal. Ces deux pratiques sont effectivement utilisées pour la vente de produits ou la promotion d'intérêts commerciaux, en incitant le client à l'achat et en usant de pression. Les fraudes téléphoniques orchestrées par des *boiler rooms* ne s'inscrivent pas uniquement dans le cadre de la fraude à l'investissement, mais peuvent également être d'autres types d'arnaques visant à escroquer de l'argent aux victimes (Fraude de « Service Canada » en 2020 par exemple (Péloquin, 2020)). Le cas de la fraude à l'investissement sera développé dans ce travail, mais les caractéristiques techniques spécifiques aux *boiler rooms* sont valables dans tous les cas.

Les *boiler rooms* peuvent être définies comme des locaux dans lesquels des groupes de fraudeurs orchestrent des fraudes en réalisant des opérations de ventes sous haute pression par téléphone. Ces locaux étaient anciennement situés dans les sous-sols d'immeubles, à proximité de la chaufferie, d'où leur nom ((Barnes, 2016; Clark, 2015; Roest, 2017). Les *boiler rooms* représentent une société d'investissements, souvent non règlementées, et réalisent ce type d'opérations dans le but de vendre des actions d'une société sans valeur ou inexistante (Clark, 2015). Ces fraudes impliquent des très grosses sommes d'argent (pouvant aller jusqu'à plusieurs millions de dollars) et de nombreuses victimes.

Que savons-nous réellement sur ces centres d'appels ? Où sont-ils situés et pourquoi ?

Il s'agit des questions de recherche auxquelles ce travail va tenter de répondre, afin de mieux comprendre ce phénomène.

Dans un premier temps, le mode opératoire typique d'une fraude à l'investissement orchestrée par une *boiler room* sera décrit. Par la suite, l'organisation globale et interne sera présentée. Pour répondre à la seconde question, l'évolution et l'état des lieux des emplacements géographiques de ces centres d'appels seront présentés, suivi d'une description des locaux utilisés.

Modus operandi

Les personnes ayant été victimes de fraudes à l'investissement ont indiqué en majorité avoir été contacté la première fois par téléphone, ce qui représente 42% d'entre elles. C'est le moyen le plus utilisé par les fraudeurs pour effectuer le premier contact, plus que par les réseaux sociaux qui représente 31% des cas (AMF, 2021).
Les investissements proposés les plus récurrents par les vendeurs sont tout d'abord les crypto-monnaies (33%), suivi de l'investissement dans l'immobilier (29%) (AMF, 2021). Mais les propositions d'investissements des fraudeurs ne se cantonnent pas à ces deux catégories. La seule limite de ce qu'ils peuvent offrir est leur imagination et peut inclure l'investissement dans des métaux rares, des diamants ou des pierres précieuses, des vins rares, etc. (Barnes, 2016).

Méthodes employées par les fraudeurs

Les compétences nécessaires pour travailler dans une *boiler room* sont très similaires de celles demandées aux télévendeurs. C'est pourquoi la plupart des fraudeurs sont des vendeurs reconvertis dans la fraude. En effet, les qualités requises sont une bonne éloquence et de la patience. Les fraudeurs sont des personnes sûres d'elles, qui ne craignent pas de mentir à leurs interlocuteurs et qui peuvent utiliser des techniques psychologiques pour les manipuler facilement et arriver à leurs fins.

Aux vues de la quantité d'appels que les vendeurs doivent effectuer, ils ont à disposition des listes de clients potentiels, dont ils savent qu'ils auront des chances d'obtenir de l'argent de leur part. Ces listes peuvent provenir de diverses sources, notamment de sources accessibles publiquement comme des annuaires téléphoniques, des listes de clients d'entreprises ou encore des noms d'administrateurs de sociétés *(FINRA, 2022)*. Ils peuvent cibler des personnes possédant déjà des actions et achèteront donc des listes d'actionnaires pour obtenir leurs noms et informations. Autrement, ils peuvent publier des publicités des magazines afin d'obtenir les noms des personnes intéressées qui y répondront. Enfin, certains n'hésitent pas à corrompre des employés dans diverses entreprises telles que des banques, des hôtels de luxe, des compagnies aériennes voire même des avocats et comptables (Drew & Cross, 2013; Financial Spread Betting, s. d.). Ils conservent ensuite ces listes et il est courant qu'elles soient échangées ou vendues à d'autres *boiler rooms* (Commission des valeurs mobilières du Manitoba, 2012).

Certains investisseurs ayant déjà été arnaqués peuvent tout à fait être appelés à nouveau car les vendeurs se servent du fait qu'une personne ayant été victime une fois a de plus grandes chances de l'être une seconde fois.

Les *boiler rooms* se définissent par des locaux d'appels d'offres sous pression où les télévendeurs utiliseront un langage persuasif et des techniques psychologiques pour pousser les investisseurs à acheter le plus d'actions possibles. Les vendeurs suscitent un sentiment d'urgence afin de ne pas laisser le temps aux investisseurs de réfléchir calmement et de se renseigner sur quel type d'actions ils s'apprêtent à acheter. Bien sûr, l'argent récolté ne sera pas investi comme indiqué au client et sera directement encaissé par les fraudeurs *(FINRA, 2022).* Lors du premier appel, les deux arguments principaux mis en avant pour pousser leurs interlocuteurs à investir sont 1) Un rendement élevé et 2) Des gains rapides. Autrement dit, ils mettront en avant le fait que le client pourra s'enrichir suite à son investissement et que ces bénéfices seront obtenus rapidement (AMF, 2021).

Afin de tromper les victimes et de les mettre en confiance, certaines *boiler rooms* possèdent des logiciels peu sophistiqués permettant de modifier le numéro de téléphone qui s'affichera sur le téléphone de l'interlocuteur. Cette méthode est appelée *spoofing*. En effet, les *boiler rooms* étant rarement dans le même pays que l'investisseur, ce programme leur permet d'afficher un numéro qui paraitra local et ainsi plus sécurisé pour l'investisseur au bout du fil (Langton, 2022; Péloquin, 2020).

D'un point de vue économique, les fraudeurs utilisent la méthode du *pump-and-dump* afin de manipuler le cours des actions d'une société à leur avantage. Cette méthode frauduleuse est très répandue et consiste à gonfler la valeur d'une entreprise qui n'en n'a en réalité pas. Pour ce faire, les vendeurs des centres d'appels achètent d'abord les actions à bas prix puis font grimper leur prix en créant tout d'abord un site web où la page d'accueil parait tout à fait sécurisée et vante la valeur de l'entreprise. Des commentaires sur le site web de prétendus investisseurs ou connaisseurs dans le domaine sont publiés, indiquant qu'il faut investir rapidement. Au téléphone, les fraudeurs informent les investisseurs que l'entreprise va bientôt entrer en bourse ou vient tout juste d'y entrer, et prétendent qu'il faut investir le plus rapidement possible. Certains iront même jusqu'à faire passer à la radio ou à la télévision des publicités concernant la société, pour rendre la tromperie encore plus légitime.

Cet engouement pousse les investisseurs naïfs à investir leur argent dans cette société sans valeur. Lorsque le cours de l'action est au plus haut, les fraudeurs cessent d'en faire la publicité, vendent leurs parts faisant chuter l'action et les investisseurs ont perdus leur argent, convaincus d'avoir fait un mauvais investissement (Roest, 2017).

Les victimes de cette fraude sont invitées à envoyer leur argent soit dans des centres financiers réputés ou sur des comptes bancaires pouvant être directement reliés à l'entreprise dans laquelle ils ont investi. En réalité, l'argent est la plupart du temps envoyé dans des comptes à l'étranger et notamment dans des paradis fiscaux comme la Suisse ou Chypre par exemple (Ralston et al., 2019; Roest, 2017).

Les différentes phases du mode opératoire

Le mode opératoire associé aux fraudes à l'investissement depuis des centres d'appels à froid peut se distinguer en quatre phases (Drew & Cross, 2013).

La première phase est celle du premier appel, effectué par le fraudeur ou « appel à froid ». Durant cet appel, l'objectif du vendeur est simplement d'établir un premier contact avec l'investisseur, de lui présenter l'opportunité que représente l'investissement et de cerner si celui-ci représente une cible d'intérêt. Il peut poser des questions à premières vue banales, comme demander l'autorisation pour envoyer des brochures sur l'investissement ou demander combien le client serait prêt à investir. Cette approche préliminaire est effectuée par des fraudeurs appelés « ouvreurs » qui sont une des deux catégories de vendeurs se trouvant dans les *boiler rooms*. A cette étape du mode opératoire, les ouvreurs prononceront simplement leur discours habituel mais n'essaieront pas d'obtenir de l'argent de la part du client (Drew & Cross, 2013).

La deuxième phase du mode opératoire est effectuée par la deuxième catégorie de fraudeurs, nommées les « fermeurs ». Ceux-ci prennent le relais et vont continuer d'appeler les investisseurs qui auront mordus à l'hameçon. A ce stade, les fermeurs vont parler plus en profondeur des spécificités du marché, s'assurer de la confirmation des documents d'investissement et vont rechercher à obtenir un engagement financier de la part du client.

La troisième phase est effectuée par le fermeur où celui-ci va continuer d'appeler régulièrement son client afin premièrement de le rassurer sur ces investissements et de lui proposer éventuellement d'autres propositions d'investissement.

Enfin, la dernière phase est celle du point de crise. Ce moment est celui où l'investisseur souhaite sortir de son investissement et de retirer ses fonds. Il est alors averti qu'il ne peut faire cela. A ce moment, les fraudeurs vont tenter de l'inciter à investir davantage ou, dans de rares cas, la victime se rendra compte de l'escroquerie (Foerch, 2022).

De manière générale, les fraudes à l'investissement sont perpétrées de préférence en période de récession économique car c'est dans ces moments que les investisseurs cherchent de nouvelles opportunités et des investissements alternatifs (Clark, 2015).

Méthodes d'ingénierie sociale

Drew et Cross (2013) ont proposé un modèle d'ingénierie sociale pour permettre de comprendre les mécanismes utilisés par les fraudeurs des locaux de vente sous pression pour obtenir de leurs victimes autant d'argent sans que ceux-ci ne s'en rendent parfois compte. Ce modèle, appelé modèle PREY considère les télévendeurs comme des prédateurs et les investisseurs comme des proies.

L'ingénierie sociale peut être définie comme « la pratique de l'acquisition d'informations par des moyens techniques et non techniques » (Manske, 2000), dont l'objectif est d'utiliser « la ruse, la persuasion, l'usurpation d'identité, la manipulation émotionnelle et l'abus de confiance pour obtenir des informations ou un accès à l'ordinateur par le biais de l'interface humaine » (Thompson, 2006).

Le modèle PREY est l'acronyme de *Profiled*, *Relational*, *Exploitable* et *Yielding*.

Profiled

La première phase du modèle PREY est celle du profilage. Avant tout appel à froid effectué par les télévendeurs, ceux-ci s'informent et profilent les clients qu'ils s'apprêtent à appeler. Ils cherchent à cette étape notamment leurs antécédents ainsi que leurs faiblesses et leurs vulnérabilités. Obtenir le plus d'informations possibles sur les investisseurs permet aux fraudeurs de présenter leur offre de façon à ce qu'elle ait l'air la plus attrayante et favorable à l'acheteur. En faisant ceci, les fraudeurs maximisent leurs chances d'obtenir une réponse positive de leur victime. Cette étape est essentielle et influencera tout le processus qui suit et le résultat final.

Relational

La seconde étape, appelée « relationnel » par les deux auteurs est perpétrée par les ouvreurs lors de l'appel à froid. Elle correspond à la première étape du mode opératoire. Les ouvreurs vont tenter par tous les moyens d'établir un lien de confiance et une relation avec leur interlocuteur. Pour ce faire, ils se servent notamment des informations obtenues antérieurement ainsi qu' « une variété de tactiques psychologiques et de techniques de persuasion » (Drew & Cross, 2013).

Les auteurs expliquent que si ces techniques psychologiques fonctionnent si bien, c'est que les victimes estiment que la plupart des gens sont honnêtes, ce qui est vrai le plus souvent. Partant de ce principe, après avoir gagné la confiance des investisseurs, ces derniers ne se méfieront plus de l'appelant.

Durant cette phase, les télévendeurs en profiteront pour convaincre de la crédibilité et de la légitimité de leur entreprise, au moyen de prospectus, sites web ou encore par la publicité.

Exploitable

L'étape de l'exploitation de la confiance peut correspondre à la deuxième et troisième phase du mode opératoire, à savoir la phase où les fermeurs prennent le relais. Les fermeurs vont alors se servir de la relation de confiance créée par leurs collègues préalablement pour tenter d'obtenir un engagement financier de leurs victimes. Ils utilisent durant ces nombreux appels des méthodes psychologiques et peuvent utiliser la peur, l'argument d'autorité voir de représailles afin de tirer avantage de la relation de confiance. Les fraudeurs peuvent notamment menacer les investisseurs de suspendre ou de violer la sécurité d'un de leur compte. Cette étape peut durer longtemps et perdurer lors de nombreux appels répétés lors desquels les fraudeurs inciteront les clients à investir davantage d'argent, tout en les rassurant sur leurs investissements précédents.

Yielding

Lorsqu'arrive le moment où l'investisseur souhaite retirer les fonds qu'il pense avoir obtenu ou simplement qu'il souhaite se retirer de son investissement, il s'agit de la dernière phase du modèle PREY : le point de crise. Les fraudeurs vont pousser les investisseurs à acheter plus d'actions, sans prendre en compte les demandes de retrait de leur interlocuteur. Ils refuseront de leurs revendre leurs actions, ou les informeront qu'ils ne peuvent pas le faire, en utilisant, comme aux étapes précédentes, le lien de confiance et des tactiques psychologiques. Il est alors très difficile pour les victimes de se rendre compte de l'escroquerie, même si ces dernières commencent à avoir des doutes.

Organisation des *boiler rooms*

Structure globale des organisations criminelles

Les organisations criminelles de *boiler room* fonctionnent de manière très complexe. Les activités sont loin d'être cantonnées à un seul centre d'appel, et impliquent un nombre important d'acteurs agissant en collaboration et dispersés dans le monde entier. En effet, le fait de travailler avec des collaborateurs présents dans divers pays du monde rends la détection de ces organisations beaucoup plus compliquée. Ce type de structure est appelée *cell-structure*, ou structure cellulaire en français, car de petites cellules ou entités interdépendantes sont dispersées à travers le monde et possèdent chacune des tâches spécifiques. Cela permet notamment que l'ensemble de l'organisation criminelle ne soit mis à mal si une ou plusieurs de ces cellules (un ou plusieurs centres d'appel par exemple) est identifiée et/ou démantelée par les autorités. De plus, de nombreux cas démontrent que les *boiler rooms* changent régulièrement de localisation pour éviter leur détection. Ainsi, identifier et démanteler une unique *boiler room* n'a pas énormément d'impact, tant ces organisations disposent de cellules à l'échelle mondiale (Roest, 2017).

L'une des règles fondamentales respectées par la majorité des *boiler rooms* est la séparation des activités administratives et des activités techniques de l'organisation. En effet, la partie technique (c'est-à-dire les centres d'appel), est le plus souvent effectuée depuis un pays différent de celui où se trouvent les dirigeants de l'organisation criminelle, qui coordonnent les actions entre les différentes cellules. Cela permet de s'assurer de la continuité des opérations en cours, et ce même si d'autres cellules de l'organisation ont été repérées par les autorités. De plus, la société d'investissement frauduleuse présentée aux victimes possède souvent une adresse dans un pays proche ou similaire au leur afin de donner plus confiance en la société d'investissement. En réalité, les *boiler rooms* étant en contact avec ces victimes ne sont la plupart du temps pas situées dans ce même pays. Pour décrire ce procédé, il est possible de mentionner le cas des *boiler rooms* espagnoles, qui représentaient environ un tiers des *boiler rooms* connues en 2009. Bien que contactant les victimes depuis le sol espagnol, les fraudeurs se faisaient en réalité passer pour une société d'investissement située ailleurs, comme au Royaume-Uni ou aux Pays-Bas.

Cette structure cellulaire offre également un gros avantage aux organisations criminelles car celles-ci peuvent profiter des différentes législations en vigueur dans les différents pays du monde. Ainsi, la localisation d'une cellule sera choisie dans un pays dont la législation lui

permettra d'effectuer ses différentes tâches avec le moins de contraintes possible. Pour reprendre l'exemple précédent, les *boiler rooms* perpétraient leurs activités en Espagne car la législation du pays ne punissait pas ce type de fraudes lorsqu'elles ne visaient pas des citoyens dans le pays. Les fraudeurs n'appelant pas de potentielles victimes situées en Espagne, ils peuvent alors continuer leurs activités sans crainte d'être appréhendés par les autorités (Barnes, 2016). Ce procédé pose des difficultés juridiques aux organisations policières luttant contre le phénomène des *boiler rooms* du fait des différentes législations régissant les pays (Roest, 2017).

Organisation interne d'une *boiler room*

Comme mentionné dans le paragraphe présentant le mode opératoire, diverses fonctions sont occupées au sein d'une organisation de *boiler rooms*. Leur nombre ainsi que leur définition varie beaucoup en fonction de la littérature, mais peuvent être présentées de cette façon :

- Les ouvreurs interviennent en premier lieu dans la fraude et vont permettre d'attirer des potentiels investisseurs. Ces ouvreurs peuvent se diviser en deux catégories : les *qualifier* qui vont effectuer les appels à froid, c'est-à-dire le premier contact avec le client, et les *verifier* qui vont rappeler certaines personnes dans le but d'attiser encore plus leur intérêt dans la société pour laquelle les actions seront vendues.
- Les fermeurs apparaissent plus tard dans le mode opératoire et peuvent être séparés en trois catégories. Tout d'abord, les *drivers* vont intervenir si les premiers ne sont pas parvenus à persuader les clients à investir immédiatement. Ils sont très doués pour faire peser une pression psychologique sur eux notamment en exposant le fait que les clients ont raté une chance inouïe d'investir dans la société mais qu'une opportunité leur est offerte pour remédier à cela. Les *coolers* vont permettre de rassurer les victimes au moment où celles-ci commencent à perdre de l'argent et qu'elles contactent donc la *boiler room* en exigeant des explications. Les *loaders* vont ensuite inciter les clients à réinvestir de l'argent au moment où le prix sera bas en les persuadant qu'ils gagneront beaucoup d'argent par la suite (Barnes, 2016; Foerch, 2022; Roest, 2017).

Comme dit précédemment, le nombre de fonctions présentes au sein d'une *boiler room* dépend notamment de sa taille. De manière générale, une cellule d'une *boiler room* est composée d'environ 20 personnes (Barnes, 2016). Là aussi, cela dépend des cas et de la taille des organisations criminelles. Le cas de *boiler rooms* en Bosnie peut notamment être cité, où un centre d'appel comptait à lui seul 40 employés. Cette *boiler room* visant des victimes

allemandes, les employés n'étaient autorisés à ne parler que l'allemand. Le bosniaque était interdit afin de maintenir l'illusion que des courtiers allemands appelaient (Roest, 2017).

Les organisations de *boiler rooms* présentent une réelle structure hiérarchique et la vie à l'intérieur est décrite par Foerch comme une « fraternité ou une version réduite de la société de courtage corrompue décrite dans Le Loup de Wall Street » (Foerch, 2022).
Les ouvreurs sont situés au niveau le plus bas de la hiérarchie. Leurs revenus sont nettement plus faibles que ceux des autres employés et varient souvent en fonction du nombre de clients qu'ils arrivent à influencer. Ces ouvreurs sont recrutés de diverses manières parmi des personnes ayant conscience ou non du fait qu'ils commettent des fraudes. Les personnes conscientes de l'illicéité de leur acte peuvent notamment être à la recherche d'une vie luxuriante, vie qui n'est en réalité pas menée par les ouvreurs. Les recruteurs vont également cibler des personnes à la recherche d'argent facile et rapide, en fournissant le moins d'efforts possibles. C'est pourquoi des ouvreurs ont déjà été embauchés sur des campus universitaires (au Royaume-Uni notamment) en proposant des jobs étudiants très attractifs, leur permettant soi-disant de gagner beaucoup d'argent tout en ayant du temps à consacrer à leurs études. Des cas en Espagne et en Asie ont également décrit des recrutements de voyageurs itinérants à la recherche d'un travail leur permettant de financer leur voyage. Beaucoup de campagnes de recrutement ont également lieu en ligne.
Ces personnes n'ont donc souvent pas conscience du fait qu'ils devront escroquer des personnes, alors qu'ils seront les premiers détectés par la police. Il est cependant compliqué de prouver leurs intentions frauduleuses (Bohen, s. d.). Les ouvreurs inconscients de la fraude offrent donc un avantage à l'organisation criminelle car s'ils se font arrêter par les autorités, ils n'auront que peu d'informations sur celle-ci à leur transmettre. De ce fait, les ouvreurs sont très souvent renouvelés au sein des *boiler rooms* (Foerch, 2022).
Bien que le statut d'ouvreur ne paraît pas très attrayant au premier abord, il est possible pour eux, dans certaines organisations, de monter des échelons hiérarchiques en guise de récompense en fonction de leurs résultats de vente. Ils peuvent notamment atteindre le statut de fermeurs (Roest, 2017).
Les fermeurs, situés plus haut dans la hiérarchie, ont tendance à plus afficher leur richesse, avec des bijoux, des costumes ou encore des voitures de luxe (Roest, 2017).

Les acteurs situés dans les échelles supérieures, tels que les hauts dirigeants de l'organisation criminelle, peuvent être amenés à contrôler plusieurs *boiler rooms* à la fois. C'est pour cette

raison qu'il est plus pertinent pour les autorités de viser les acteurs hautement situés dans la hiérarchie dans une optique de répression. Démanteler une unique cellule n'aura pas forcément d'impact significatif dans la continuité des opérations de l'organisation, surtout si celle-ci opère à l'international.

Collaborateurs

Fausse société

L'organisation des activités d'une *boiler room* ne se fait pas uniquement au sein de celle-ci. De fausses sociétés interviennent également dans cette fraude. Les *boiler rooms* ont d'ailleurs pour but de vendre des actions de cette entreprise. Il s'agit la plupart du temps d'une fausse entreprise, créée par des fraudeurs, se faisant passer pour légitime et souhaitant chercher des investisseurs. Parfois, à défaut de créer une fausse entreprise de toute pièce, les fraudeurs peuvent racheter une entreprise ayant fait faillite à prix très abordable. Cette pratique peut avoir des avantages, notamment pour obtenir une cotation en bourse bon marché et de contourner la procédure de souscription à la cote d'une bourse qui est longue et complexe (Financial Spread Betting, s. d.). De plus, si les individus sont déjà connus comme commettant des fraudes, leur inscription en bourse peut être compliquée. Si les *boiler rooms* sont souvent situées dans un pays différent de celui des victimes, les fausses sociétés vont plutôt avoir tendance à présenter une adresse située dans le même pays, afin d'ajouter un sentiment de confiance aux victimes dans l'entreprise dans laquelle elles vont potentiellement investir.

Les fraudeurs de la *boiler room* et de la compagnie peuvent être les mêmes individus, ce qui facilite d'ailleurs grandement la coordination des actions. Cependant, les fraudeurs possédant des fausses sociétés peuvent également employer des *boiler rooms* existantes afin de faciliter la vente d'actions frauduleuses et partager un certain pourcentage du gain.

Enfin, il peut également arriver que certaines entreprises légitimes, ayant des difficultés à vendre leurs actions, emploient des *boiler rooms* sans le savoir, pensant qu'il s'agit d'une société d'investissement légitime. Des actions frauduleuses peuvent alors débuter sans volonté de la société en question.

Autres collaborateurs

De la même façon qu'avec les fausses sociétés, les *boiler rooms* peuvent collaborer avec des professionnels, ce qui a notamment pour but de légitimer leur entreprise et la vente d'actions. Il peut s'agir de créateur de sites web, d'experts-comptables, d'agents de règlement ou encore

d'avocats. Ces professionnels ont les capacités techniques de détecter ce genre de schémas frauduleux. Ainsi, on peut imaginer que ces collaborateurs sont, la plupart du temps, pleinement conscient qu'ils collaborent avec des fraudeurs, et que leur nom est utilisé à ces fins. Les agents de règlement collaborant avec des *boiler rooms* leur permettent d'ouvrir plus facilement des comptes bancaires et d'effectuer des transactions d'argent provenant de l'escroquerie sans attirer de soupçons (Roest, 2017). Les avocats vont, quant à eux, permettre d'apporter des conseils juridiques ou encore de rédiger des documents officiels. Ils peuvent également servir de fiduciaire, c'est-à-dire de gérer les fonds obtenus par l'organisation, si ces fonds sont envoyés dans des paradis fiscaux par exemple (Roest, 2017).

Ainsi, en collaborant avec des *boiler rooms*, les personnes occupant ces fonctions rendent les entreprises plus légitimes aux yeux des futures victimes et facilitent donc la vente d'investissements frauduleux (ils peuvent être vus comme des facilitateurs de la fraude) (Barnes, 2016; Roest, 2017). De plus, ces facilitateurs permettent également de blanchir les fonds obtenus grâce à la fraude.

Il peut arriver que des sociétés d'investissements soient également des *boiler rooms* et réalisent des actions légales et illégales parallèlement. Dans ce cas, le personnel y travaillant est composé de courtiers qui sont également des fraudeurs impliqués dans une organisation criminelle de *boiler rooms*. Cela offre de nombreux avantages à l'organisation criminelle car les locaux sont ainsi loués au nom de la société de courtage et les bureaux sont d'ores et déjà meublés (Roest, 2017).

Les *boiler rooms* collaborent également avec des *recovery room* qui commettent une autre forme de fraude apparaissant après la première. Ces *recovery room* vont notamment appeler des victimes de *boiler rooms* et leur offrir la possibilité de recouvrer l'argent perdu. Ces *recovery room* peuvent contenir les mêmes personnes que dans les *boiler rooms*, ou être en lien avec celles-ci afin de faciliter la communication des informations des victimes escroquées.

Les liens entre ces différents collaborateurs sont présentés à la page suivante (voir figure 1).

Cette organisation en cellule a certes des avantages mais apporte également son lot d'inconvénients. En effet, comme ces facilitateurs ont souvent des activités légales en parallèle des activités frauduleuses, cela augmente la possibilité de traçage de ces facilitateurs, et donc du réseau criminel. Ainsi, la structure des organisations de *boiler rooms* est délibérément rendue complexe, dans le but de retarder au maximum leur identification et leur démantèlement par les autorités. Elles ont également recours à des contre-mesures dans ce même but. Les cellules de *boiler rooms* sont amenées à changer constamment de localisation. Des moyens technologiques

de plus en plus sophistiqués sont utilisés afin de de dissimuler les communications ou leur position GPS. De plus, l'usage de violence est évité et la corruption avec d'autres acteurs est limité pour ne pas attirer l'attention. Les identités réelles des personnes sont tenues secrètes la plupart du temps, et les personnes y travaillant utilisent des fausses identités (Roest, 2017).

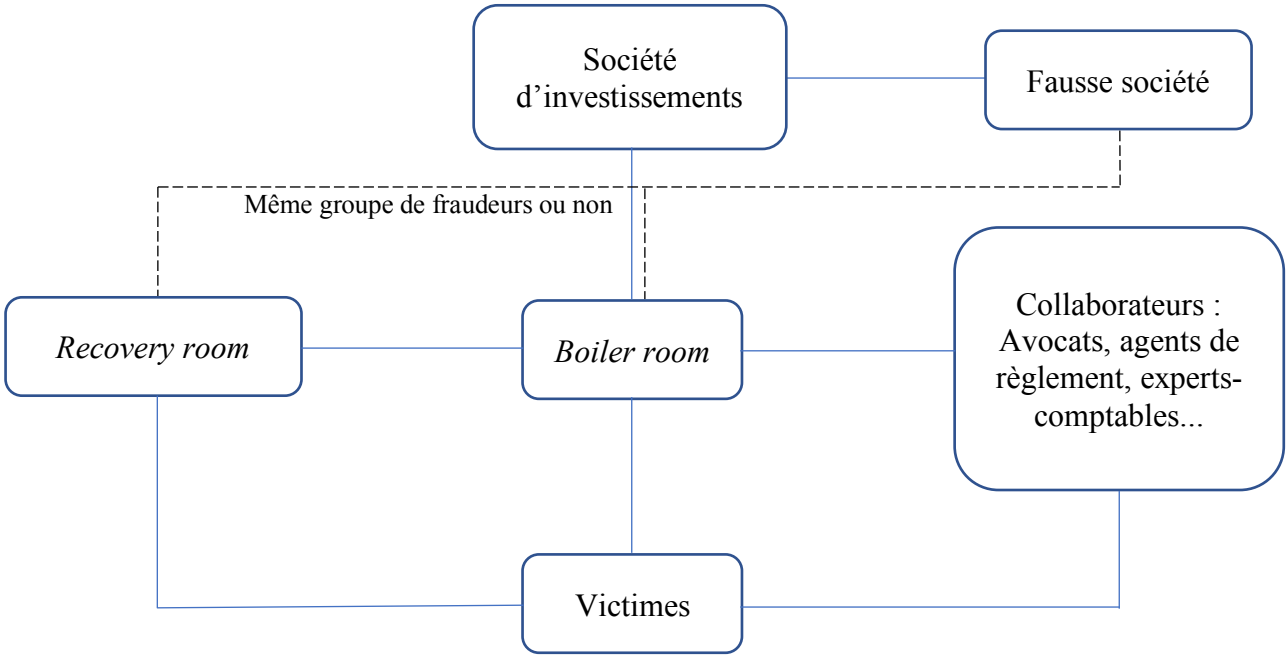

Figure 1 : Acteurs impliqués dans une fraude de type boiler room

Localisations géographiques des *boiler rooms*

Localisation à l'échelle mondiale et continentale

A l'échelle mondiale aujourd'hui, des *boiler rooms* se trouvent sur tous les continents. En Europe, elles se concentrent principalement en Espagne et certaines se trouvent en Europe de l'Est. En Asie, les *boiler rooms* se situent surtout en Asie du Sud-Est. Beaucoup d'entre elles sont localisées aux Philippines et les *boiler rooms* situées en Thaïlande, en Indonésie et en Malaisie représentent des opérations plus petites. Sur le continent africain, les locaux de vente sous pression se trouvent de plus en plus en Afrique du Sud (Financial Spread Betting, s. d.). En Australie, la Gold Coast du Queensland à la réputation d'être la capitale australienne de la fraude à l'investissement et comprend de nombreuses *boiler rooms* actives (Robertson, 2015).

Les *boiler rooms* ne se trouvent pas forcément sur le même continent que les investisseurs qu'elles ciblent. C'est notamment le cas de Michael Newman, ayant fraudé plus de 9,4 millions de livres sterling à des investisseurs qui habitaient au Royaume-Uni, en Australie et en Nouvelle-Zélande, depuis des *boiler rooms* situées au Laos (Telegraph and Argus, 2003).

Les *boiler rooms* qui visent des investisseurs situés en Europe se trouvent pour la plupart en Espagne et en moindre mesure en Europe de l'Est. De la même manière, les investisseurs en Asie ou en Océanie sont appelés par des *boiler rooms* localisées en Thaïlande, aux Philippines, au Cambodge, ou au Laos (Barnes, 2016).

Dans le cas spécifique du Royaume-Uni, sur les neuf affaires pénales ayant concernées des victimes de fraude à l'investissement par des *boiler rooms* depuis 2009, sept d'entre elles comprenaient des *boiler rooms* situées en Espagne. Une affaire comptait des *boiler rooms* en Irlande et une où les locaux étaient probablement situés aux Caraïbes. Parmi ces affaires, certains fraudeurs prétendaient appeler depuis Francfort, Stockholm ou encore Amsterdam (Barnes, 2016).

Origine des *boiler rooms*

Les premiers locaux de vente sous pression prennent racine dans les années 1920 en Floride, aux États-Unis.
Cette décennie, caractérisée par une période de prospérité était également celle d'une forte croissance économique. L'augmentation de la production industrielle a permis aux entreprises de s'enrichir et aux investisseurs de faire des crédits pour acheter des actions en masse. Parallèlement, la fraude à l'investissement s'est également développée et avec le téléphone qui était considéré à l'époque comme un outil peu cher pour faire du marketing, les premières *boiler rooms* ont vu le jour (Clark, 2015; McMahon et al., 2013).

Évolution des localisations des *boiler rooms* des années 1920 à nos jours

Alors qu'originellement les *boiler rooms* situées aux États-Unis ciblaient des investisseurs américains, à partir des années 1920, la croissance économique des États-Unis s'est rapidement déportée outre Atlantique. Les fraudes perpétrées dans des *boiler rooms* en Floride ont tout de même perdurées pendant sept décennies (McMahon et al., 2013).
Dans les années 2010, de nombreuses *boiler rooms* situées aux États-Unis et au Canada ont déplacés leurs locaux à l'étranger à « Hong Kong, aux Bahamas, en Thaïlande, au Panama, au Costa Rica, en Europe (de l'Est) et en Afrique du Sud » (Roest, 2017).

Le fait que les fraudeurs choisissent ces emplacements plutôt que d'autres n'est pas sans raison. Premièrement, ils privilégient les pays qui n'ont pas de contrats d'extradition avec les pays des investisseurs qu'ils souhaitent cibler. Cela leur permet d'éviter ou de limiter les risques de procédure judiciaire dans le pays où se trouvent les victimes. A la fin du XX^{ème} siècle, certains fraudeurs ciblant des investisseurs aux États-Unis opéraient depuis Montréal, Toronto ou Vancouver profitant du fait que l'extradition vers les États-Unis prenait des années et que la justice au Canada était laxiste à ce niveau (Schneider, 1997).
Deuxièmement, les fraudeurs vont préférentiellement s'implanter où les législations sur le télémarketing leurs sont favorables. En effet, les législations sont différentes dans chaque pays et ont des définitions différentes de ce qui est légal et illégal, notamment en ce qui concerne les pratiques de démarchage téléphonique (Roest, 2017). Par exemple, au Royaume-Uni depuis 2007, il est interdit « pour les entreprises basées au Royaume-Uni d'appeler à froid un investisseur pour tenter de vendre des actions » (Police Scotland, 2021).

Les changements de localisations des locaux de vente sous pression peuvent également s'expliquer par les opérations de démantèlement menées par les autorités d'un pays. Au Canada, en septembre 2005, le bureau de la concurrence a démantelé de nombreuses *boiler rooms*, à Toronto et à Calgary. Les autorités canadiennes et américaines ont procédé aux arrestations des fraudeurs de ces locaux (Gouvernement du Canada, 2005).

De manière générale, les *boiler rooms* seront implantées dans des pays où les autorités ne s'intéressent pas ou peu à cette problématique. De plus, ils séparent les lieux d'emplacement des *boiler rooms*, de ceux des investisseurs qu'ils ciblent et du lieu d'envoi des fonds pour brouiller les pistes et tirer avantage des failles et limites du système juridique international. Ils préfèrent également les pays ou les autorités locales peuvent facilement être soudoyées et où les peines sont faibles (Barnes, 2016).

A l'échelle européenne, au milieu du XX^{ème} siècle, les boilers rooms se trouvaient notamment au Royaume-Uni et aux Pays-Bas. En 1980, l'endroit le plus populaire pour établir des locaux de vente sous pression était Amsterdam. Mais les polices locales ont fourni des efforts de démantèlement de ces locaux, qui se sont avérés efficaces localement. Malheureusement, cette lutte contre les *boiler rooms* à l'échelle locale ne permettent pas de venir à bout de ce problème mais uniquement de le déplacer. C'est pourquoi aujourd'hui, la plupart des *boiler rooms* européennes sont situées en Espagne (Barnes, 2016).

Le Royaume-Uni se démarque particulièrement en matière de prévention et d'actions entreprises pour lutter contre la fraude à l'investissement et les *boiler rooms*.
Elle dispose de différentes organisations permettant de prévenir la population du risque que celle-ci représentent. La FSA/FCA (*Financial Services Authority / Financial Conduct Authority*) est chargée de réguler les marchés financiers au Royaume-Uni et publie régulièrement des listes des entreprises connues pour offrir des services illégaux. Ces listes sont mises à jour dès que les autorités ont connaissance de nouvelles entreprises frauduleuses. La National Fraud Authority (NFA) lancée en 2009, est une organisation gouvernementale de lutte contre la fraude. Fermée en 2013, elle a été remplacée par *Action Fraud* et est située au sein de la police de Londres (Barnes, 2016; Roest, 2017).
Des organisations de prévention et de lutte contre la fraude se retrouvent dans de nombreux pays comme la Belgique, les Pays-Bas et également à l'échelle européenne et mondiale (Roest, 2017).

Deux opérations policières ont permis de lutter efficacement contre l'organisation des *boiler rooms*. En 2007, l'opération Archway a été lancée par la police de la ville de Londres qui a mis en place un système de signalement de fraudes liées aux *boiler rooms*. Cette opération a permis à la police de récolter de nombreux renseignements et de coordonner leurs efforts pour lutter contre ces locaux (Barnes, 2016).

En 2015, la Police de la ville de Londres a lancé une nouvelle opération appelée opération Broadway dont l'objectif était de coordonner les efforts pour s'attaquer aux *boiler rooms* en tant qu'organisation criminelle. Cette opération a regroupé plusieurs agences (telles que la FCA, les *National Trading Standards*) pour lutter contre le crime organisé. Cette coordination à grande échelle a permis de démanteler de nombreuses *boiler rooms* situées dans différents quartiers de la ville. Cette opération est toujours utilisée et est « une composante importante de la stratégie globale » de la Police de Londres pour lutter activement contre le crime organisé (Action Fraud, 2015).

Type de locaux

Historique et évolution

À l'origine, le terme « *boiler room* » provient des locaux dans lequel s'installaient des groupes de fraudeurs, situés dans les bas étages d'immeubles, souvent à proximité des chaufferies (Clark, 2015). Durant le XX^{ème} siècle, les fraudes de *boiler rooms* étaient effectivement perpétrées depuis ce genre de pièces. Celles-ci contenaient le plus de bureaux (disposés en ligne) et de téléphones possibles dans un espace restreint, les fraudeurs disposant donc de très peu de place (U.S Securities and Exchange Commission, s. d.). Contrairement aux idées reçues, les immeubles dans lesquels s'installent les *boiler rooms* peuvent être très prestigieux. Cela permet de rajouter une impression de légitimité à la société d'investissement, et donc d'inciter les personnes à investir (Action Fraud, 2015; Roest, 2017).

Par la suite, à partir des années 1990, les locaux de *boiler rooms* se sont agrandis pour ressembler de plus en plus à ce que le cinéma a pu montrer dans les films sur le sujet. Les grands *open-spaces*, présentés dans les films « *Boiler Room »* de Ben Younger (2000) et « *The Wolf of Wall Street* » de Martin Scorsese (2013), ont été de plus en plus utilisés par les groupes de fraudeurs, notamment aux États-Unis. Ce fut notamment le cas d'une *boiler room* basée à Woodland Hills en Californie, où dans une salle au rez-de-chaussée d'un immeuble se trouvaient entre 35 et 45 postes informatiques disposés en ligne. Dans ce même cas, chaque rangée de postes informatiques était composée de trois ou quatre ouvreurs donnant des pistes à un fermeur situé au bout de la rangée (Foerch, 2022). Les ouvreurs devaient passer l'entièreté de leur journée au téléphone et étaient renvoyés si ce n'étaient pas le cas.

Cependant, ce type de *boiler room* est de moins en moins observé depuis quelques années. Les autorités des pays concernés ce sont de plus en plus intéressées au phénomène ce qui a permis de faire évoluer la législation, et ce notamment aux États-Unis qui disposait d'un nombre important de *boiler rooms* (Policastro & Payne, 2014; Shover et al., 2004).

Devenant les cibles de lourdes procédures de régulation, les fraudeurs n'ont eu d'autres choix que d'imaginer de nouvelles formes de *boiler rooms*, et d'abandonner leurs locaux aux aspects cinématographiques (Tierney, 2021). Ainsi, de nouvelles techniques ce sont mises en place pour échapper à ces régulations. La technique du *rip-and-tear* est notamment apparue au sein des *boiler rooms* (Policastro & Payne, 2014). Cette technique consiste à utiliser des « bureaux-mobiles », c'est-à-dire d'effectuer les fraudes depuis des lieux qui changent constamment, afin

de réduire les possibilités de se faire arrêter par la police. De ce fait, les groupes de fraudeurs s'improvisent des bureaux dans des chambres d'hôtels ou dans des locaux loués sous de faux-noms (Clark, 2015; Slotter, 1998). De la même façon, les fraudeurs peuvent être amenés à utiliser des téléphones jetables et des cartes prépayées afin de pouvoir appeler depuis n'importe où sans se faire repérer (Fraud Guides, 2014; Shover, 2005; Tzani-Pepelasi et al., 2020). L'aménagement de ces « bureaux-mobiles » est fait très rapidement et de manière minimaliste, afin de disposer du strict nécessaire pour mener à bien leurs opérations. Cela inclus donc au minimum des bureaux et des téléphones (Roest, 2017). Parfois, d'autres éléments peuvent être retrouvés comme des appareils de *spoofing* (permettant de modifier le numéro de téléphone s'affichant à l'écran) (Bohen, s. d.; Commission des valeurs mobilières du Manitoba, 2012). En outre, la technique du *rip-and-tear* implique plusieurs actions fondamentales, en plus du changement de localisation. Les fraudeurs vont privilégier l'argent liquide et peuvent demander aux victimes d'effectuer des transactions en envoyant l'argent à des boîtes postales. L'argent liquide est en effet beaucoup plus difficile à tracer par les autorités (Barnes, 2016; Fraud Guides, 2014).

Les groupes de fraudeurs ont ainsi démontré une grande adaptabilité au fil des années pour faire perdurer leurs activités malgré les évolutions en matière de régulation des autorités.

Prévention et répression

Au Royaume-Uni, suite à de nombreux rapports de *Action Fraud* et du *National Fraud Intelligence Bureau*, l'opération Broadway a été mise en œuvre en 2015. En effet, il a été estimé que plus de 1.73 milliard de livres sterling avaient été perdues par 5252 investisseurs dans des fraudes de type *boiler room* au Royaume-Uni. De nombreuses *boiler rooms* étaient situées dans des immeubles prestigieux de la ville de Londres et chacune gagnait, en moyenne, 1.25 million de livre (Action Fraud, 2015).

Dans le cadre de l'opération Broadway lancée par les *City of London Police, City of London Trading Standards* et *Metropolitan Police*, un groupe de travail entre plusieurs agences a mis en évidence plusieurs signes pouvant être caractéristique de la présence d'une *boiler room* dans un lieu. Le but était principalement de mettre en garde les organismes louant des pièces ou des bureaux que leurs locaux pouvaient être utilisés pour commettre ce type de fraude et les inciter à s'intéresser davantage aux activités de leurs locataires. Les signes caractéristiques ont également été partagés avec l'ensemble de la population londonienne, notamment les personnes

travaillant dans les gros immeubles de la ville, pour que ceux-ci puissent transmettre du renseignement aux organisations policières. En plus de démanteler les *boiler rooms*, le but de cette opération était également d'éduquer l'ensemble des personnes à identifier ces groupes de fraudeurs avant qu'ils ne gagnent de l'argent sur le dos des victimes (Action Fraud, 2015)
Les différents signes caractéristiques de la présence de *boiler rooms*, partagés lors de l'opération sont les suivants :

- Les locaux sont loués pour une courte période et avec de l'argent liquide.
- Les horaires de travail des employés sont inhabituels.
- Le nom de la société d'investissements n'est pas écrit à la réception de l'immeuble.
- Les employés utilisent de faux-noms pour eux-mêmes et pour l'entreprise.
- Les employés passent beaucoup de temps à lire des scripts (Action Fraud, 2015).

Cette opération a été la plus grande opération de répression perpétrée dans un pays. En effet, les autres États ont surtout axé leur message de prévention au niveau des victimes potentielles, en présentant les comportements typiques des fraudeurs. L'opération Broadway apporte une approche beaucoup plus proactive en ciblant les locaux abritant des *boiler rooms*, ce qui pourrait permettre d'identifier ces groupes de fraudeurs avant même qu'ils n'aient pu commencer à lancer leurs appels.

Discussion

Il a été vu au cours de cette étude que les fraudeurs ont changé leur implantation à plusieurs reprises pour continuer leurs actions illicites malgré les nombreux efforts des autorités. Cela indique que ces activités frauduleuses doivent être particulièrement attractives et qu'ils ne sont pas prêt de les arrêter. Il est donc facile d'imaginer que les groupes de fraudeurs vont continuer de se diriger vers les pays dont la législation réprime peu ce phénomène.

Ces difficultés poussent les pays à axer leur politique de prévention sur les victimes plutôt que sur les groupes criminels. En effet, dans de nombreux pays ont été créées des organisations spécialisées dans la lutte contre la fraude. Ces organismes proposent pour la plupart des aides aux victimes et des conseils pour leur apprendre à détecter des appels frauduleux et éviter de se faire avoir.
Depuis 2019, les opérateurs canadiens proposent des techniques de blocage de numéros suspicieux, suite aux directives de la CRTC. Ce dispositif peut également s'avérer utile pour protéger la population canadienne des appels provenant de *boiler rooms*.

Outre les méthodes utilisées par les fraudeurs pour éviter les autorités vues précédemment, les fraudeurs vont privilégier des domaines de l'investissement qui sont les moins réglementés, c'est-à-dire tous les nouveaux types d'investissement parmi lesquels peuvent être comptés les crypto monnaies ou de plus en plus les NFT (Barnes, 2016).
Toutes ces astuces utilisées par les fraudeurs rendent difficile le travail des autorités du pays dont la population est victime car elles ne peuvent pas intenter d'actions répressives sur les *boiler rooms* situées à l'étranger. De plus, lorsque les fraudeurs sont identifiés dans le pays hébergeant la *boiler room*, en l'absence de loi d'extradition, les auteurs ne pourront pas être livré dans le pays dans lequel il devront être jugés.

Au cours de cette étude, il a été vu que des opérations de démantèlement ont d'ores et déjà été effectuées dans quelques pays. Cependant, comme dans le cas des Pays-Bas, cela peut certes permettre de supprimer les *boiler rooms* dans une région, mais les cellules seront surtout délocalisées dans d'autres pays, ce qui ne permet pas de venir à bout de ce phénomène durablement. Les *boiler rooms* sont inscrites dans des organisations criminelles internationales et doivent être considérées comme une structure complexe et non pas comme des locaux indépendants. Les opérations les plus fructueuses seraient donc celles qui s'attaquent aux *boiler*

rooms en tant qu'organisation, et qui ciblent les personnes coordonnant ses activités. Ces opérations nécessiteraient de coordonner les efforts des autorités et d'agences spécialisées dans la lutte contre la fraude pour s'attaquer à la source, c'est-à-dire les dirigeants des groupes criminels. Cette approche, plus proactive, permettrait également de s'attaquer aux *boiler rooms* avant qu'elles n'aient pu gagner de l'argent sur le dos de leurs victimes.

Conclusion

Différents stratagèmes et techniques sont utilisées par les fraudeurs pour obtenir de leurs victimes le plus d'argent possible. Qu'il s'agisse d'astuces sur le plan économique comme le *pump-and-dump* pour manipuler les actions ou de méthodes psychologiques inspirées de l'ingénierie sociale. Le mode opératoire pratiqué par les fraudeurs consiste à obtenir les informations nécessaires sur un potentiel investisseur avant le premier contact afin de lui présenter l'offre de la façon la plus attrayante pour lui. Le moment où ce dernier voudra récupérer ses actions sera saisi par les fraudeurs comme nouvelle opportunité pour lui soustraire de l'argent.

Loin de la vision d'un petit local étant le berceau de nombreuses de fraudes, les *boiler rooms* s'insèrent en réalité dans de véritables organisations, à la manière d'une entreprise. Une hiérarchisation se créé entre les ouvreurs et les fermeurs, effectuant les opérations techniques, et les dirigeants qui gèreront l'ensemble des activités tout en restant en retrait des centres d'appels. De nombreux collaborateurs sont impliqués dans ces fraudes, tels que des avocats, des experts-comptables, des agents de règlements... Ils auront des rôles de facilitateurs de la fraude en facilitant notamment la réalisation de tâches administratives (ouverture de compte, conseils juridiques...). Ces collaborateurs leurs seront également d'une grande aide pour blanchir les fonds obtenus grâce à la fraude.

Originellement localisées aux États-Unis dans les années 1920, les *boiler rooms* se sont développées et délocalisées pour être situées aujourd'hui sur tous les continents. Ces déplacements sont guidés par les changements de législations et les opérations policières mises en place pour démanteler ces locaux. Les *boiler rooms* sont aujourd'hui principalement concentrées en Asie du Sud-Est et en Espagne dans le cas de l'Europe.

Même le choix des locaux est organisé de manière à éviter au maximum la détection par les autorités. Des évolutions sur ce point ont pu être constatées et sont notamment dues à l'apparition de lois de régulation dans les pays d'Amérique du Nord par exemple. Les groupes de fraudeurs ont changé de locaux pour se situer, actuellement, dans des bureaux minimalistes et aménagés rapidement. Ces bureaux peuvent être des chambres hôtels ou des locaux loués sur une courte période. Tout est fait pour pouvoir partir le plus rapidement possible et laisser un minimum de traces de leur passage.

L'enjeu pour venir à bout de ces *boiler rooms* est de coordonner les opérations de polices sur la scène internationale. Pour ce faire, les *boiler rooms* doivent être considérées comme des organisations complexes et non comme de petites cellules agissant localement.

Bibliographie

Action Fraud. (2015, mars 18). *Op Broadway—Multi-agency drive to stop investment fraud in the Capital*. Action Fraud. https://www.actionfraud.police.uk/news/op-broadway-multi-agency-drive-to-stop-investment-fraud-in-the-capital

AMF. (2021). *Les Français et les arnaques à l'investissement*.

Barnes, P. (2016). Stock market scams, shell companies, penny shares, boiler rooms and cold calling : The UK experience. *International Journal of Law, Crime and Justice*, *48*, 50-64. https://doi.org/10.1016/j.ijlcj.2016.11.001

Bohen, T. (s. d.). *What Is a Boiler Room Operation—And Is It Illegal?* StocksToTrade. Consulté 19 décembre 2022, à l'adresse https://stockstotrade.com/boiler-room-operation/

Centre antifraude du Canada. (2021). *Rapport annuel 2021*.

Clark, D. (2015). *Tracking the victims of Boiler-room Fraud—Citizenz at risk !* [Master]. Université de Cambridge.

Commission des valeurs mobilières du Manitoba. (2012). *Les opérations de vente sous pression—Risquez-vous d'en être victime?* https://mbsecurities.ca/get-informed/pubs/boiler_fr.pdf

Drew, J. M., & Cross, C. (2013). Fraud and its PREY : Conceptualising social engineering tactics and its impact on financial literacy outcomes. *Journal of Financial Services Marketing*, *18*(3), 188-198. https://doi.org/10.1057/fsm.2013.14

Financial Spread Betting. (s. d.). *Boiler Rooms and Recovery Room Scams*. Consulté 9 décembre 2022, à l'adresse https://www.financial-spread-betting.com/Boiler-Room-Scams.html

FINRA. (2022, avril 6). *Boiler Rooms—An Old Stock Scam Gets a Technology Makeover*. https://www.nasdaq.com/articles/boiler-rooms-an-old-stock-scam-gets-a-technology-makeover

Foerch, A. (2022, août 15). *Dial for gold : Inside California's precious metals 'boiler rooms'*. Sjo3ekt.Js. http://citywire.com/ria/news/dial-for-gold-inside-california-s-precious-metals-boiler-rooms/a2394792

Fraud Guides. (2014, décembre 8). Rip and Tear Schemes. Fraud Guides. https://www.fraudguides.com/telemarketing/rip-tear-schemes/

Gouvernement du Canada. (2005, septembre 27). *Le Bureau de la concurrence participe au démantèlement d'opérations de vente sous pression* [Communiqués de presse]. https://www.canada.ca/fr/nouvelles/archive/2005/09/bureau-concurrence-participe-demantclement-operations-vente-pression.html

Langton, J. (2022, mars 16). *B.C. fraudster found running Colombian boiler room, SEC alleges*. https://www.advisor.ca/news/industry-news/b-c-fraudsman-found-running-colombian-boiler-room-sec-alleges/

Manske, K. (2000). An Introduction to Social Engineering. *Information Systems Security*, *9*(5), 1-7. https://doi.org/10.1201/1086/43312.9.5.20001112/31378.10

McMahon, R. J., CLI, & CFE. (2013). *Practical Handbook for Professional Investigators, Third Edition* (3rd edition). CRC Press.

New York Southern District Court. (2019). *USA v. Ralston.*

Péloquin, T. (2020, août 31). Fraude de service canada, pour une arnaque, faites le 1. *La Presse*

Policastro, C., & Payne, B. K. (2014). *Can You Hear Me Now Telemarketing Fraud*. https://doi.org/10.1007/s12103-014-9279-x

Police Scotland. (2021). *Boiler room fraud*. https://www.scotland.police.uk/advice-and-information/scams-and-frauds/boiler-room-fraud/

Ralston, R., Wright, C., & Hooper, S. (2019). *UNITED STATES OF AMERICA*.

Robertson, J. (2015, août 17). *'The biggest mistake in my life' : How Gold Coast boiler room scams duped investors*. The Guardian. https://www.theguardian.com/money/2015/aug/17/the-biggest-mistake-in-my-life-how-gold-coast-boiler-room-scams-duped-investors

Roest, F. (2017). *Share Fraud & Boiler Room Scams Exposed*.

Schneider, H. (1997, août 24). *Telemarketing Scams Reach Across Borders*. The Washington Post. https://www.washingtonpost.com/wp-srv/inatl/longterm/canada/stories/telemarket082497.htm

Shover, N. (2005). *Telemarketing Predators : Finally, We've Got Their Number*. National Institute of Justice. https://nij.ojp.gov/topics/articles/telemarketing-predators-finally-weve-got-their-number

Shover, N., Coffey, G. S., & Sanders, C. R. (2004). Dialing for Dollars : Opportunities, Justifications, and Telemarketing Fraud. *Qualitative Sociology*, *27*(1), 59-75. https://doi.org/10.1023/B:QUAS.0000015544.69646.f1

Slotter, K. (1998). Hidden faces : Combatting telemarketing fraud. *FBI L. Enforcement Bull. 9*.

Telegraph and Argus. (2003, novembre 17). *Man loses £23,000 in world-wide scam*. https://www.thetelegraphandargus.co.uk/news/8007415.man-loses-23000-in-world-wide-scam/

Thompson, S. T. C. (2006). Helping the Hacker? Library Information, Security, and Social Engineering. *Information Technology and Libraries*, *25*(4), Art. 4. https://doi.org/10.6017/ital.v25i4.3355

Tierney, J. F. (2021). Investment Games. *Duke Law Journal*, *72*.

Tzani-Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R., & Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos : Offender Characteristics. *Journal of Forensic and Investigative Accounting*, *12*(1).

U.S Securities and Exchange Commission. (s. d.). Top Tips for Your Readers. http://www.sec.gov/investor/links/toptips.htm

Walker, R. H. (2000). SEC Testimony : Organized Crime on Wall Street. 15.