UNIVERSITÉ DE MONTRÉAL

De Forex à crypto : Revue des modus operandi derrière les fraudes à l'investissement

PAR

SHANNA AUGER-DROLET

ISABELLE CHADIC

ÉCOLE DE CRIMINOLOGIE

FACULTÉ DES ARTS ET DES SCIENCES

TRAVAIL PRÉSENTÉ À MADAME MASARAH PAQUET-CLOUSTON

DANS LE CADRE DU COURS CRI-6228

CRIMINALITÉS ÉCONOMIQUES

20 DÉCEMBRE 2022

TABLE DES MATIÈRES

ABSTRACT

Ce travail porte sur une revue des fraudes à l'investissement liées aux arnaques sur les marchés du Forex et de la cryptomonnaie. Un recensement des modus operandi de ces types d'arnaques démontre que les fraudeurs se servent du sentiment de confiance et utilisent principalement des véhicules technologiques tels que les réseaux sociaux pour effectuer leurs crimes. Par ailleurs, une analyse victimologique indique un bassin de victimes varié, mais dont quelques facteurs de vulnérabilités sont communs tels une faible connaissance en investissement et un désir d'effectuer rapidement des gains monétaires. Finalement, les mesures de prévention proposées se basent sur le Protection Motivation Theory de Rogers (1975), cadre théorique axé sur la proactivité des victimes. Les mesures se fondent entre autres sur l'exposition aux risques, l'éducation financière et la technologie.

INTRODUCTION

Le domaine de l'investissement est composé de différents marchés permettant le profit aux citoyens désireux d'assurer leur avenir ou tout simplement de maintenir un niveau confortable. Malheureusement, là où il y a des occasions de faire un gain, se présente aussi des opportunités criminelles pour les fraudeurs. Dans les dernières années, il a été possible d'observer une recrudescence des fraudes à l'investissement. (Radio-Canada, 2022) Bien que ces escroqueries soient toujours en vigueur, l'engouement autour du marché de la cryptomonnaie et celui du Forex a également attiré les fraudeurs à mettre en place divers stratagèmes malveillants (Coin,L, J., 2022 ; Malinga, 2020). L'appât du gain facile et la promesse de rendements très élevés convainc plus d'un individu à investir (Coin,L, J., 2022). De même, les fraudeurs sont très habiles à manipuler la technologie afin de soutirer de l'argent aux victimes (AMF, 2022). En ce sens, des véhicules technologiques tels que les réseaux sociaux sont utilisés par ces acteurs malveillants à titre d'outil facilitateur de leurs crimes. D'ailleurs, les plus populaires auprès de ces derniers sont Télégram, Whatsapp, Instagram et Facebook (Coin,L, J., 2022).

Par ailleurs, cette problématique fait des victimes à travers le monde entier. En Amérique du Nord, le Centre antifraude du Canada rapporte qu'en 2021, plus de 40% des pertes financières seraient dues aux fraudes à l'investissement. (Centre antifraude du Canada, s.d). Plus précisément, les pertes associées aux fraudes à la cryptomonnaie s'élevaient à 75 millions de dollars (Banque Nationale du Canada, 2022). Aux États-Unis, le rapport de *Federal Trade Commission* mentionne que près de la moitié des personnes qui ont voulu investir dans le marché des cryptomonnaies ont perdu de l'argent à cause d'une arnaque en 2021 pour un total de plus de 1 milliard de dollars (Coin,L, J., 2022). Du côté de l'Europe, l'Autorité des marchés financiers en France expose que ces mêmes fraudes représentaient plus du quart de la totalité des arnaques recensées (Ibid). En ce qui concerne le marché du Forex, la prépondérance des fraudes n'a pas été explicitement statuer par les organismes chargés de recenser ce type de statistiques . Or, les montants associés aux pertes sont également impressionnants. Par exemple, un homme en Alberta a perdu plus de 550 000 dollars canadiens dans ce type de fraude (Abdel-Qader, 2020).

Dû à l'ampleur de la problématique, nous nous sommes penchées sur les stratagèmes utilisés par les fraudeurs en fonction des marchés d'investissements. À cet effet, la présente recherche fera état des modus operandi des arnaques reliés à la cryptomonnaie et au Forex. Afin d'arriver à nos résultats, nous avons recensé les écrits sur le sujet autant au niveau scientifique qu'en sources ouvertes pour d'exploiter la richesse des détails disponibles sur les stratagèmes. L'objectif général de notre recherche consiste à comprendre les différents schémas frauduleux afin d'améliorer la réponse à ce type de crime. Subséquemment, nous avions également pour but de découvrir s'il existe une transition dans les techniques frauduleuses entre les deux marchés en établissant un profil comparatif de leurs similitudes et de leurs différences. Finalement, nous nous sommes également intéressées à la victimologie afin de faire la proposition de solutions préventives prometteuses afin de contrer ce phénomène.

PARTIE 1 : PRÉSENTATION DES ÉLÉMENTS ÉTUDIÉS

1.1 Qu'est ce que le Forex ?

Le FOREX (« Foreign exchange market » ou « FX market ») est le marché mondial d'échange de devises étrangères (Kumar, 2014 ; Jackson et Curry, 2022; Glantz et Kissel, 2014). L'action elle-même d'échange sur le marché du Forex (« Forex trading ») implique l'achat et la vente simultanées de deux devises nommées paires de devises (Kumar, 2014; Melvin et Norbin, 2017; Li, 2016). Par exemple, EUR/USD , USD/JPY, GBP/USD, désignées commes " les majeures" représentent les trois paires de devises les plus échangées au monde (Kumar, 2014). D'ailleurs, cette caractéristique centrale de l'échange des devises trouve son sens dans le désir d'équilibrer les différents facteurs agissant sur les devises entre deux pays par l'établissement d'un taux de change qui, lui, représente la valeur de ces paires. (TD Ameritrade, 2018). Bref, le marché Forex détermine les valeurs relatives des différentes devises et permet leur conversion (MBN ; Jackson et Curry, 2022).

Représentant le plus grand marché financier au monde, le FX market possède un rôle notable dans l'économie (Melvin et Norrbin, 2017). En effet, le commerce d'échange de devises est particulièrement nécessaire en ce qui trait au tourisme, à l'achat et la vente de différents biens et d'investissements au niveau international (Melvin et Norrbin, 2017; MBN, s.d). Par exemple, le Forex est d'utilité pour un gouvernement qui prend la décision de faire des affaires avec un autre pays et qui doit ainsi convertir sa devise en celle du pays étranger (TD Ameritrade, 2018). De même, un simple voyageur qui désire échanger des devises, par exemple, canadienne (CAD) en américaine (USD), effectue une transaction sur le marché du Forex (Li, 2016).

Comme cité par les exemples ci-dessus, le FX market est utilisé à des fins pratiques. Néanmoins, la majorité des échanges de devises sont effectuées afin de réaliser un profit (Glanz et Kissel, 2014). En effet, le Forex est également utilisé par les banques (centrales, d'investissement et commerciales), les Hedge funds, les courtiers de détail et les investisseurs qui vont eux aussi acheter et vendre des devises étrangères en spéculant sur les variations des prix des différentes devises (Ibid.). Ce rendement est réalisable en raison de la forte volatilité du marché, soit une très grande variation des prix des négociations (Admirals, 2022). Étant ouvert

24h/24, 5 jours sur 5, la marché Forex est marqué par un très haut volume transactionnel faisant fluctuer les prix des devises et définit en fonction de l'offre et la demande (TD ameritrade, 2018 ; Jackson et Curry 2022).

Toutefois, Melvin et Norrbin (2017) note que le FX market serait dominé par les grandes banques commerciales situées dans le monde entier qui procèdent aux échanges de devises sur le interbank market : « Les géants possède des activités à l'échelle mondiale qui leur permettre des cotations compétitives sur un grand nombre de devis" (Melvin et Norrbin, 2017). Hormis le fait que ce marché soit strictement réservé aux institutions bancaires, il représente l'influence première, à court terme, des taux de change à travers le monde (Staszkiewicz et Staszkiewicz, 2015 ; CFI, 2022). Divers facteurs macroéconomiques influencent également le taux de change tels que les taux d'intérêt, le rythme de la croissance économique et l'environnement politique des différents pays (Jackson et Curry, 2022 ; Drake, 2021). Les événements majeurs tels que des guerres ou des catastrophes naturelles représentent aussi inévitablement un facteur d'impact économique pour un pays influençant le prix de sa devise (Drake, 2021 ; IG, s.d). De même, le sentiment du marché des différents investisseurs peut également influencer le prix des devises dont les pressentiment sont souvent reliés aux événements énoncés plus haut (Ibid).

Un marché décentralisé

Kumar (2014) et Melvin et Norrbin (2017) partagent une représentation intéressante du Forex le décrivant comme un réseau de différents acteurs connectés par des systèmes informatiques et téléphoniques dans le but d'y faire l'échange de devises. Cette dernière évoque le caractère décentralisé qui émane du FX market soit une structure différente de celle du marché boursier (Delage et al., 2011). À l'opposé de ce dernier où les offres d'achats et de ventes passent par une unité centrale qui traite l'ensemble transactions, le Forex n'est pas contrôlé par une seule agence ou gouvernement et les différents investisseurs à travers le monde ne sont pas tous soumis aux mêmes réglementations (Delage et al. 2011; Li, 2016). Plus précisément, le Foreign exchange Market est qualifié de marché gré à gré (OTC market) où la négociation se fait directement entre les acheteurs et vendeurs (MBN ; Melvin et Norrbin, 2017; Delage et al. 2011; Kumar, 2014).

Au Canada, le Forex trading est supervisé par l'OCRCVM (Organisme canadien de réglementation du commerce des valeurs mobilières) tel un titre ou un dérivé, ce qui varie selon les législations provinciales (CSA, s.d). En ce sens, les régulateurs locaux de chaque province faisant partie des autorités canadiennes en valeur mobilières (ACVM) ont le pouvoir d'agréer un courtier (Uchino, 2022). Par exemple, au Québec, il s'agit de l'Autorité des marchés financiers et, en Ontario, la Commission des valeurs mobilières de l'Ontario (Ibid.). Ainsi, toute entreprise ou particulier qui désire faire l'offre de services de Forex trading doivent être enregistrés auprès de la province auxquels ils désirent mener leurs activités, de même qu'être membre de l'OCRCVM (CSA, s.d; Ucchino, 2022). Plusieurs plateformes en ligne sont offertes afin d'accéder au marché Forex (Staszkiewicz et Staszkiewicz, 2015) et d'obtenir les services d'un courtier en ligne (Trading view, s.d). Or, cette avancée ouvre également une porte vers aux risques que comporte le marché FOREX pour les fonds des investisseurs inexpérimentés.

1.2 Qu'est -ce que la cryptomonnaie ?

Avant d'élaborer sur les modus operandi derrière les fraudes à l'investissement, il est important de comprendre ce qu'est la cryptomonnaie. En fait, ce type de monnaie est un actif numérique, soit virtuel (Banque Nationale du Canada, 2022). Parmi les monnaies les plus connues sur le marché des cryptomonnaies, se trouve le Bitcoin et l'Ethereum (Ibid). Par le fait même, le marché de ces cryptoactifs se retrouve sous l'échange de la monnaie virtuelle contre certains biens et services dont sa valeur peut fluctuer telle une action en bourse (Ibid). Toutefois, la cryptomonnaie est reconnue pour être plus instable que les actions cotées en bourse (Ibid.). De plus, la création et les transactions de cryptomonnaies dépendent de la technologie des «blockchains» qui permet quant à elle le principe de minage (Revenu Québec, 2022). Les cryptomonnaies sont donc préservées dans un portefeuille de cryptomonnaies numérique possible grâce à un hachage cryptographique contenant une valeur (Astrakhantseva & al., 2021). D'ailleurs, soulignons que le marché des cryptomonnaies est qualifié de décentralisé, et donc la monnaie virtuelle s'échange par le pair à pair sur des plateformes d'échanges en ligne (Banque Nationale du Canada, 2022). Il n'y a donc pas une entité centrale qui gère ce marché.

Parallèlement, le marché des cryptomonnaies est ciblé par les fraudeurs en raison des vulnérabilités qu'il comporte. Premièrement, il s'agit d'une nouvelle technologie qui n'est presque pas encadrée par les autorités gouvernementales ou réglementaires (Berecz, s.d). En effet, son caractère décentralisé rend complexe l'imputabilité en cas de fraude (Ibid). Deuxièmement, le marché des cryptomonnaies permet d'effectuer des transactions dans l'anonymat, ce que la monnaie courante ne permet pas (Banque Nationale du Canada, 2022 ; Berecz, s.d). Troisièmement, représentant une certaine complexité technique, beaucoup d'individus intéressés à investir dans ce domaine ne possèdent pas les connaissances techniques (Berecz, s.d). En ce sens, les investisseurs inexpérimentés deviennent plus à risque de mordre à l'hameçon des personnes mal intentionnées qui se présument expert dans le domaine (Ibid.). Quatrièmement, son caractère numérique le rend sensible aux dangers de l'internet : quelques compétences malveillantes sont suffisantes pour mettre à exécution les stratagèmes frauduleux (Ibid). Finalement, les cryptomonnaies sont irréversibles c'est-à-dire qu'il n'est pas possible d'annuler une transaction, par exemple, Ethereum et donc un paiement frauduleux ne sera pas remboursé (Ibid.)

PARTIE 2 : REGARD SUR LES MODUS OPERANDI

2.1 Modus operandi de la fraude reliée à au marché Forex

Le marché du Forex est ciblé par les fraudeurs qui cherchent à exploiter les vulnérabilités inhérentes de sa structure. D'une part, le fait qu'il s'agit d'un marché décentralisé et que les transactions soient effectuées au moyen de l'informatique (Staszkiewicz et Staszkiewicz, 2015) offre des opportunités exponentielles aux fraudeurs où de nombreuses cibles intéressantes sont accessibles et dont les risques de se faire arrêter sont moindres (Boccadutri, 2020). Même si le FX market est réglementé au Canada, plusieurs fraudeurs font acte de présence sur le web et échappent aux contrôles des autorités (Ibid.). D'autre part, la complexité du marché Forex demande un certain niveau de connaissance, dont plus investisseurs s'engagent trop rapidement sans avoir acquis le savoir requis. (Giambrone, s.d).

Les prochaines sections feront état des différents modus operandi utilisés dans la commission de fraudes sur le marché du Forex.

2.1.1 Les vendeurs de signaux , les robots Forex et le marketing d'affiliation

Agissant à titre de vendeur indépendant ou œuvrant pour une compagnie, les fraudeurs tentent de vendre à des individus désireux d'investir dans le Forex des informations dites expertes (Hope, 2022). Ces dernières indiqueraient aux investisseurs les moments précis où vendre et acheter des devises étrangères afin d'en tirer le maximum de profits. (Giambrone, s.d ; Hope, 2022). Afin de renforcer leur crédibilité, les criminels soutiennent que leurs informations sont générées par des études de marché menées par des professionnels garantissant les prévisions annoncées (SFLCN, 2022; Giambrone, s.d ; Jendruszak, 2022). De plus, pour rendre le tout d'apparence légitime, les fraudeurs vont offrir de faux témoignages de soi-disant investisseurs qui auraient bénéficié du service (Giambrone, S.D). Dans un laps de temps rapproché suivant l'adhésion au service, les clients reçoivent généralement lesdits signaux par courriel ou texto les informant qu'il est temps d'effectuer une transaction (Finance magnates, 2022). À un moment défini par le fraudeur, ce dernier coupera la communication avec les clients (Ibid.). Puisque le service est facturable, la fréquence des paiements varient d'un fraudeur à l'autre : quotidien, hebdomadaire, mensuelle, etc. (Giambrone, s.d). Ainsi, certains fraudeurs vont choisir de soutirer des plus petits montants à la fois faisant perdurer la fraude dans le temps. D'autres vont plutôt demander un paiement plus important et dans certains cas, disparaîtront, sans même offrir le service (SFLC, 2022). Au final, les fraudeurs s'emparent des fonds des individus, tout en leur offrant des informations fabriquées de toutes pièces qui n'ont aucune utilité réelle afin de réaliser un gain (Jendruszak, 2022; Giambrone, s.d).

Une variante de cette arnaque est également identifiée sous les services de robots Forex (Jendruszak, 2022 ; Hope, 2022). Les fraudeurs font la promesse aux intéressés que leurs robots sont programmés afin de prendre en charge les transactions, le tout ayant un taux de précision et d'efficacité de 100% (Hope, 2022). D'ailleurs, la plupart de ces faux robots FOREX ne possèdent même pas ledit logiciel, ce qui le rend tout simplement non fonctionnel (Ibid.). Malgré

tout, certains bots Forex légitimes existent et sont utilisés par des professionnels afin de mener des analyses techniques : évaluation des performances passées, identification de grandes tendances, etc. (Hope, 2022; Finance magnates, 2022 ; Giambrone, s.d). Certes, il ne sont pas infaillibles et ne peuvent prédire le marché comme l'annoncent les fraudeurs (Ibid.).

Parallèlement, la vente de ces faux services est également utilisée lors d'un stratagème subséquent, soit le marketing d'affiliation frauduleux. D'une base tout à fait légale, il s'agit d'une méthode permettant de gagner un revenu par une commission, en aidant une entité (personne ou compagnie) à vendre ces produits ou services (HEC, 2022). Dans le cas de la fraude Forex, le caractère frauduleux de cette pratique émane de deux sous-stratagèmes. Le premier modus operandi consiste à ce que l'employé-vendeur offre, gratuitement ou à moindre coûts, un robot Forex à un potentiel investisseur à condition de contracter les services d'un courtier spécifique, soit son patron (Avatrade, s.d). Lorsque la victime adhère à la demande, elle reçoit un robot non fonctionnel, perd potentiellement les fonds déboursés pour le produit, de même que se fait dérober son investissement par le courtier qui s'avère frauduleux (Watkins, 2018). De plus, pour le criminel qui sollicite les cibles, ce dernier se voit offrir une commission (Ibid.). Il s'agit donc d'un stratagème organisé conduisant non seulement à une victimisation répétée chez les investisseurs, mais également un double gain pour les fraudeurs dont la valeur du gain criminel dépend de leur rôle dans la commission de la fraude. Dans le deuxième modus operandi, les fraudeurs invitent les intéressés à s'inscrire au programme d'affiliation sur une plateforme frauduleuse (Ibid,). Ces derniers feront la recherche d'investisseurs potentiels, mais la commission ne leur sera jamais remise, alors que d'autres victimes recrutées par l'employé victimisé placeront des fonds chez les courtiers frauduleux (Ibid.). Ainsi, les faux courtiers arnaque à la fois son "employé" de même que les victimes attirées par ce dernier.

2.1.2 Escroqueries aux faux courtiers Forex et plateformes frauduleuses

Non réglementés, de faux courtiers approchent des investisseurs inexpérimentés ou en déficit de temps afin de leur offrir de gérer leurs investissements sur le Forex (Jendruszak, 2022). Ces derniers promettent à ces potentiels clients des offres alléchantes et non réalistes telles que

des promotions et bonus incroyables (AMF, s.d). La plupart d'entre eux vont également assurer des rendements garantis, quasi-impossible à prévoir en raison de la forte volatilité du marché (Hope, 2022; Boccadutri, 2020). Afin de paraître légitime, les fraudeurs réalisent une certaine préparation préalable au contact telle que la fabrication de documents administratifs crédibles à faire compléter à la victime (AMF, s.d; AMF, 2021). L'un des préparatifs primordial au bon fonctionnement du stratagème est la création d'une plateforme frauduleuse ou l'usurpation du nom d'un courtier Forex enregistré (Jendruszak, 2022 ; Hope, 2022).

En effet, ces criminels copient non seulement le nom et l'interface web, mais également le numéro d'enregistrement d'une société afin de gagner la confiance des internautes (Hope 2022; Boccadutri, 2021). De cette façon, lorsqu'un potentiel investisseur à la recherche d'une plateforme effectue quelques vérifications sur sa légitimité, il pourrait y retrouver la société comme enregistré sur un site de réglementation (Ibid.). D'ailleurs, les plateformes frauduleuses sont diffusées aux potentielles victimes par différentes stratégies telles les pubs sur les réseaux sociaux et moteurs de recherche (Boccadutri, 2020). Or, certains faux courtiers opèrent par téléphone à partir de boiler room situé à l'étranger (AMF, s.d). D'autres peuvent même agir via des stratagèmes de fraudes amoureuses (CFTC, s.d). Par exemple, un fraudeur approchera sa victime via un réseaux social ou un site de rencontre tel Tinder afin d'établir une relation amicale ou amoureuse, servant d'appât pour l'attirer à investir auprès d'une plateforme frauduleuse Forex (CFTC, s.d)

Le stratagème débute par l'incitation à ouvrir un compte auprès de la plateforme frauduleuse en y déposant des fonds par carte de crédit, prépayé ou virement bancaire (AMF, s.d). Les faux courtiers utilisent un langage technique afin d'étourdir les victimes et les inciter les victimes à déposer des sommes de plus en plus importantes (Ibid.). Entre-temps, les fraudeurs vont méticuleusement construire une relation amicale avec le client afin d'établir un lien de confiance pouvant outrepasser la remise en question de leurs services (Boccadutri, 2020 ; AMF, 2021). Il s'agit donc un aspect important du stratagème qui assurera également une longévité de la fraude (Ibid.). Quelque temps après l'adhésion des victimes aux services des faux courtiers, les fraudeurs vont chercher à rassurer leurs clients en les informant d'un retour en investissement (Jendruszak, 2022) . Malgré cela, à un certain moment, les victimes vont prendre connaissance de la fraude puisqu'il ne sera pas possible de retirer ledit investissement (Ibid.). Par conséquent,

les fraudeurs coupent le contact en rendant les fonds inaccessibles pour la victime (Giambrone, s.d). D'ailleurs, le détournement de fonds finance les achats personnels des courtiers représentant souvent des produits de luxe (Giambrone, s.d ; Jendruszak, 2022).

Ce modus operandi se retrouve également sous les faux fonds communs de placements qui s'inspirent du modèle traditionnel des fonds spéculatifs, mais qui sont gérés par des gestionnaires non réglementés (Avatrade, s.d). Pour attirer les investisseurs, les fraudeurs promettent des rendements gonflés, mais demandent des frais de gestion excessifs (Ibid.). Le même modus operandi que décrit ci-haut s'ensuit (Ibid).

2.1.3 Les manipulations techniques frauduleuses

Certains courtiers ne se contentent pas de soutirer directement des sommes à leurs clients, mais s'adonnent à des manipulations subtiles sur leurs propres plateformes de trading Forex. L'une de ces manœuvres concerne les bid/ask spreads des paires de devises sur le FX market. Dans ce stratagème, un courtier frauduleux augmente l'écart (*spread*) entre le taux affiché sur le marché Forex et le taux à débourser réellement par l'investisseur afin d'augmenter son profit de façon exagérée (Giambrone, s.d). Normalement, l'écart est d'environ de 2 à 3 pips ce qui représente 2 à 3 centièmes de pourcentage du prix d'achat de la paires de devises, alors que l'arnaque implique de 7 à 8 pips (Ibid.).

En outre, une autre manipulation frauduleuse s'apparentant au délit d'initié appelée le "front running" est également effectué par certains courtiers. Cette pratique illégale se manifeste lorsqu'un client demande à son courtier d'effectuer une transaction importante sur le marché des devises (FXCM, 2018). Or, ce dernier utilise cette information afin d'effectuer lui-même une transaction avec son compte personnel concernant la même paire de devises demandée par son client (Ibid). De cette façon, le courtier profite de la future hausse de la valeur de la paire suivant l'achat de la transaction de devises qu'il effectuera subséquemment pour son client (Ibid.). Ainsi, cette manipulation désavantage monétairement l'investisseur au détriment de son courtier, dans le mesure où il paiera la paire de devises à un prix plus élevé (Ibid.).

2.1.4 Les stratagèmes de Ponzi Forex et la vente pyramidale

Sans surprise, ces stratagèmes populaires dans le domaine criminel des fraudes à l'investissement se retrouvent également sur le marché Forex. L'autorité des marchés financiers définit la fraude Ponzi comme l'utilisation de sommes remises par un investisseur à un groupe de trading afin de payer de faux rendements à d'autres investisseurs ou à titre de somme de remboursement pour ceux qui désirent récupérer leur fonds (AMF, s.d). Lorsque le nombre d'investisseurs est à la baisse, les fraudeurs vont généralement disparaître ou ne plus répondre aux différentes demandes de retraits des investisseurs (Ibid).

Plus particulièrement, dans l'environnement Forex, les escrocs se font passer pour un groupe d'investissement ou une société de gestion de comptes disposant d'une plateforme de trading Forex (Jendruszak, 2022; Finance Magnates, 2022). Ces derniers promettent aux investisseurs des rendement élevés sans risque en investissant une toute petite somme initiale (Giambrone, S.D). Lorsque les victimes y adhèrent, les fraudeurs demandent aux victimes de débourser des frais supplémentaires, de même que de procéder au recrutement d'autres investisseurs (Jendruszak, 2022). Les prochains investisseurs recrutés par ces derniers seront demandé de suivre les mêmes étapes, et ainsi de suite (Ibid.). Comme prévu par le classique stratagème de vente pyramidale, le recrutement est une excuse utilisée par les fraudeurs mentionnant que les profits seraient en augmentation au fur et à mesure que le nombre d'investisseurs accroît (AMF, s.d).

Dépendamment de l'individu malveillant, certains fraudeurs effectuent un versement à titre de retour en investissement, généré par les fonds des autres victimes et ce, pour deux raisons (Giambrone, s.d, Jendruszak, 2022). La première étant de rendre d'apparence légitime le stratagème, la deuxième étant de motiver les investisseurs arnaqués à faire du recrutement pour amplifier les gains finaux à dérober (Ibid.). En effet, lorsque la participation aux stratagèmes décroît, les criminels disparaîtront avec les fonds investis de tous (Ibid.). D'ailleurs, ce stratagème peut également être utilisé afin de dérober des fonds par un stratagème secondaire soit la vente de services (signaux, vidéos, formations) fabriqués de toute pièce alimentant la cagnotte finale (Finance Magnates, 2022).

2.1.5 Les faux gourous Forex

Du côté des influenceurs frauduleux, les réseaux sociaux représentent le cœur de leur stratagème. En effet, ces derniers publient sur leurs comptes Instagram, Tiktok et autres des images d'eux démontrant un style de vie luxueux et ce, afin d'attirer l'attention des utilisateurs : jets privés, voitures et vêtements de luxe, etc. (Ucchino, 2022 ; AMF, 2021). Vendeur de rêves, ces faux gourous centrent leurs récits autour du concept de la liberté financière se traduisant par le fait d'être riche et à la retraite dans sa trentaine (AMF, 2021). Parallèlement, ces derniers véhiculent que leur fortune est due à de connaissances aiguisées du Forex trading (Ucchino, 2022). Par conséquent, afin d'obtenir le même niveau de vie, ces derniers font l'offre de cours extrêmement dispendieux afin d'apprendre aux investisseurs la façon dont faire des investissements sur le Forex (Ibid). Envieuses d'un mode de vie à faire rêver, les victimes déboursent le prix de ces formations qui sont en réalité, basé sur des faits inventés (Ibid). Prenons le cas de l'influence thaïlandaise nommée "Nutty" qui aurait convaincue 6 000 personnes d'investir dans le Forex afin de vivre dans le luxe tout comme elle (Bloomberg, 2022). Nutty a promis à ses abonnées des rendements atteignant 35% en suivant ces formations, alors que ces dernières étaient frauduleuses, faisant perdre plus de 30 millions de Baht aux victimes, soit environ 1 170 000 $ canadiens (Ibid.).

2.1.6 Les faux avocats Forex

Ce type d'arnaque diffère de celles présentées ci-dessus, puisqu'elle cible les victimes préalablement touché par des fraudes Forex. Dans un premier temps, les fraudeurs repèrent une victime de fraude Forex sur un forum de discussion ou dans des groupes de soutien sur les réseaux sociaux tel que Facebook (Boccadutri, 2021). Lorsque ces derniers choisissent leurs victimes, ils procèdent à un premier contact par téléphone, courriel ou message privé d'un quelconque réseau, en se présentant comme un avocat dont l'expertise est dirigée vers le recouvrement d'argent volés par de faux courtiers Forex (Ibid). Afin d'amadouer les victimes, ces derniers vont généralement affirmer, que le service est gratuit et qu'un faible paiement pourrait être exigé lorsque les fonds seront récupérés (Ibid). Une fois les victimes en confiance, les arnaqueurs vont laisser s'écouler quelque temps afin de faire croire qu'ils ont travaillé sur le

dossier. Lors du deuxième contact, ces derniers vont informer leurs victimes que leurs fonds ont été restitués avec succès. Malheureusement, ces fonds seraient bloqués sur un compte bancaire situé à l'étranger accessible seulement par un dépôt d'argent. Certains fraudeurs vont se contenter d'un paiement, alors que d'autres vont en demander plusieurs en fonction de la vulnérabilité de la victime (Ibid). En bref, nous assistons à une victimisation répétée où les fonds des victimes seront dérobés de nouveaux par les faux avocats (Ibid.). Notons également que certains de ces faux avocats ne perdent pas de temps et demandent directement des fonds pour débloquer les dites sommes volées lors d'un premier appel (Ibid.).

2.2 Modus operandi de la fraude reliée à au marché de la cryptomonnaie

Les modus operandi des fraudes liées à la cryptomonnaie se fondent sur deux aspects. D'un côté, les fraudeurs utilisent des techniques d'ingénierie sociale où des manipulations psychologiques sont perpétrées afin d'obtenir des renseignements (Astrakhantseva & al., 2021) De l'autre côté, les fraudeurs tentent de gagner la confiance des individus afin de leur soutirer des fonds (Ibid). Lorsque les victimes ont des doutes, les fraudeurs pourront jouer sur cette relation afin de les rassurer et les encourager à leur remettre des sommes via des stratagèmes frauduleux (Ibid.). Toutefois, lorsque celles-ci voudront retirer leur argent, les criminels trouveront différentes excuses pour ne pas leur rendre la somme investie et disparaîtront avec leurs plateformes (Ibid.).

Les sections suivantes feront état des différents schémas mis en œuvre par les fraudeurs afin de maximiser les rendements de leurs crimes.

2.2.1 La fraude de l'offre d'emploi

Ce stratagème survient lorsque les fraudeurs se font passer pour des recruteurs à la recherche de personnes désirant travailler dans le domaine de la cryptomonnaie (Banque Nationale du Canada, 2022). Tout d'abord, les fraudeurs vont publier une offre d'emploi très intéressante, mais dont l'embauche nécessite que les individus paient leurs formations

obligatoires en cryptomonnaies (Ibid). Ces offres sont partagées par le moyen de publicités qui relatent que les formations présentent des conseils sur comment effectuer un taux de rendement très haut, pratiquement surréaliste (AMF, 2022). Afin d'inciter les individus à sauter sur l'occasion, les fraudeurs vont faire la promesse qu'ils deviendront des experts très rapidement (Ibid.). Par ailleurs, le stratagème est mis en place afin que les victimes déboursent de plus en plus de fonds au fil du temps, tel que pour des formations subséquentes ou autres dépenses liées à l'emploi (Ibid.). Or, les fonds seront dérobés par les fraudeurs et il ne sera pas possible de les récupérer (Banque Nationale du Canada, 2022). Tel que rapporté par l'AMF, les jeunes sont particulièrement intéressés par ce type d'emploi qui offre une forme d'éducation alternative « Les jeunes abonnés se voient proposer un savoir qui "ne s'apprend pas à l'école" : un contenu opérationnel, activable, véritablement utile dans une perspective de réussite financière. » (AMF, 2022).

2.2.2 La fraude des faux sites d'investissement

Tel que le marché du Forex, le marché de la cryptomonnaie est également touché par le phénomène des plateformes d'échange frauduleuses. Ce modus operandi s'installe lorsque les fraudeurs tentent d'influencer le maximum d'individus à utiliser leurs plateformes (Banque Nationale du Canada, 2022). Ces derniers utilisent des promesses de rendements extraordinaires ou encore de rabais sur de haut taux de frais de transaction à débourser sur les sites légitimes (Ibid). La plupart des fraudeurs font usage des réseaux sociaux comme Facebook, Instagram et Tik Tok pour attirer leurs victimes (Daniel, 2022). D'ailleurs, certains vont même jusqu'à engager des influenceurs sur les réseaux sociaux pour faire la promotion de leur fausse cryptomonnaie (Ibid.). Une fois que les victimes effectuent des transactions sur les faux sites, celles-ci perdent automatiquement l'argent investi car les montants vont directement dans le portefeuille des fraudeurs (Ibid.). Plusieurs exemples vécus permettent d'illustrer ce stratagème. Prenons le cas d'un homme septuagénaire québécois qui a été attiré par une publicité sur un réseau social faisant promotion d'une plateforme de cryptomonnaie frauduleuse. Après avoir investi et observé une hausse de la somme de son portefeuille, celui-ci a voulu retirer son argent. Lorsque le supposé courtier financier a commencé à trouver des justifications pour ne pas lui

rendre son argent, l'homme à réalisé qu'il s'était fait arnaqué pour plus d'un million de dollars (Radio-Canada, 2022).

2.2.3 La fraude du transfert des crypto-monnaies

Cette fraude s'apparente aux stratagèmes présentés ci-dessus. Cependant, elle se distingue par le transfert des cryptomonnaies d'une plateforme à une autre et non un simple investissement de devises à une monnaie virtuelle. En premier lieu, les fraudeurs incitent les individus à se procurer de la cryptomonnaie sur une plateforme légitime (AMF, 2022). Par la suite, une fois la relation de confiance établie, les fraudeurs vont tenter de convaincre les victimes d'effectuer un transfert de leurs cryptomonnaies vers une autre plateforme afin d'augmenter leurs rendements (Ibid.). Or, la deuxième plateforme est une plateforme frauduleuse dont les rendements affichés sont faux (Ibid.). Une fois les cryptomonnaies transférées, celles-ci seront tout simplement volées par les fraudeurs (Ibid).

2.2.4 La fraude du stratagème de placement

Cette fraude est également similaire aux deux stratagèmes précédents. En revanche, celle-ci se distingue par le sentiment d'urgence auprès de la victime, mentionnant que l'opportunité offerte est limitée (AMF, 2022). En ce sens, les fraudeurs invitent les victimes à investir dans un type de cryptomonnaie qui aurait des rendements spectaculaires et sans risque. En effet, le marché de la cryptomonnaie permet avec facilité la création de nouveaux jetons de cryptoactifs (initial coin offering (ICO) (Ibid). Plusieurs plateformes d'échange décentralisées permettent la mise en marché de ces nouveaux jetons sans avoir besoin d'une quelconque autorisation. Ceci engendre donc un environnement qui se rend favorable à la fraude (Ibid). Des manipulations de type Pump and Dump sont également observables où des individus malveillants font la promotion d'une cryptomonnaie afin d'inciter les gens à investir (Ibid). Lorsque le prix de celle-ci devient élevé, les fraudeurs se retirent laissant les investisseurs à perte (Ibid). Finalement, étant donné le besoin de trouver constamment de nouvelles victimes, ce type de fraude incitent également les fraudeurs à utiliser des systèmes pyramidaux comme les

systèmes Ponzi pour inciter les victimes à effectuer du recrutement dans ce stratagème de faux investissement (Banque Nationale du Canada, 2022).

2.2.5 La fraude amoureuse-amitié

Ce modus operandi prend place lorsque des individus malveillants contactent des victimes par l'utilisation de faux profils sur des réseaux sociaux ou sites de rencontre tel que Tinder (Autorité des marchés financiers 2022). Les fraudeurs établissent une relation de confiance en s'intéressant particulièrement à la victime (ce qu'elle préfère, ses passe-temps) de même que par le partage de faux intérêts communs. Une fois la relation bien établie, les fraudeurs changent la direction de la conversation vers le sujet d'investissement sur le marché des cryptomonnaies. Afin de rendre le tout alléchant, les criminels expriment qu'ils ont effectué de haut rendements à la suite de ces investissements (Ibid.). Par la suite, les fraudeurs offrent la possibilité d'investir en cryptomonnaies via la même plateforme qui les ont rendu aisés. Une fois le premier montant investi par les victimes, les malfaiteurs leur en demandent toujours plus jusqu'au jour où ils s'enfuient avec l'argent et la plateforme disparaît (Ibid.). Ce stratagème est populaire auprès des fraudeurs en cryptomonnaies : en 2021 le Centre antifraude du Canada a recensé plus de 457 victimes canadiennes qui ont perdu de l'argent dans une fraude amoureuse liée à de la cryptomonnaie, ce qui représente une perte d'environ 40 millions de dollars (La Tribune, 2022). En 2022, plus de 189 victimes ont été également recensées reliées à ce type de fraude, ce qui constitue un montant de 18.3 millions de dollars (Ibid.).

2.2.6 La fraude de la récupération de l'argent perdu

Ce type de fraude est caractérisé par une victimisation répétée. Lors de ce modus operandi, les fraudeurs ciblent explicitement les victimes d'une précédente fraude à l'investissement liés à la cryptomonnaie ayant vécues la perte d'une somme d'argent (AMF,

2022). À cet effet, les fraudeurs prennent contact avec leurs cibles afin de leur proposer de l'aide en regard de la récupération de leurs pertes lors de la fraude antérieure (Ibid). Toutefois, une fois l'argent envoyé au fraudeur, aucun service n'est fourni et le fraudeur coupe tout contact (Ibid).

PARTIE 3 : ANALYSE DES MODUS OPERANDIS SUR LES DIFFÉRENTS MARCHÉS

3.1 Similitudes des modus operandis

Nous observons que les schémas des fraudes commises sur les marchés du Forex et de la cryptomonnaie reposent sur les mêmes principes. En effet, le fondement des délits associés aux fraudes à l'investissement se base sur des caractéristiques telles que la confiance, une forte dépendance aux ressources du fraudeur et l'influence social (Lacey et al., 2020) que l'on retrouve dans les modus operandi sur les deux marchés. Parallèlement, nous pouvons constater une multiplicité des stratagèmes pour chaque type de marché, de même que certains schémas types qui sont utilisés autant dans les fraudes de Forex que dans le domaine de la cryptomonnaie. Par exemple, nous notons l'utilisation de plateformes frauduleuses, de stratagèmes de ventes pyramidales et de fraudes amoureuses ainsi que ceux reliés au remboursement de sommes perdues par les fraudeurs oeuvrant sur les deux marchés.

Puis, les deux marchés sont décentralisés et utilisent la technologie pour accomplir leurs opérations quotidiennes. Bien que le Forex existait avant l'ère d'internet, l'utilisation de la technologie, à permis une plus grande exposition au public et également à transformer les façons de faire des transactions (Paxful, 2020). La cryptomonnaie quant à elle existe grâce à la technologie (Ibid.). En ce sens, les transactions liées aux deux marchés se font par le moyen de la technologie, représentant le point tournant de la perte de fonds. Ainsi, cette caractéristique des marchés rend plus facile la finalisation du modus operandi en dupant certains investisseurs qui ne possèdent pas les connaissances techniques, mais offre également un plus plus grand bassin de cibles potentielles aux fraudeurs.

Nous pouvons donc remarquer qu'il y a une récurrence dans les schémas d'arnaques qui étaient très populaires auprès de Forex, qui est désormais appliquée à la cryptomonnaie. Masama (2021) explique ce déplacement en partie en raison que le Forex est désormais réglementé dans

plusieurs pays du monde. L'avènement de la cryptomonnaie propose un marché également très volatile, ce qui vient offrir une nouvelle opportunité d'investir dans un marché très peu réglementé (Ibid.) et conséquemment ouvrir l'opportunité aux fraudeurs d'appliquer les stratagèmes de fraudes qui sont utilisés dans le Forex à celui des cryptomonnaies.

3.2 Les différences des modus operandis

À la suite de la revue des modus operandi à l'égard des deux marchés étudiés, nous remarquons certaines différences entre les stratagèmes du Forex et celui de la cryptomonnaie. Au niveau du Forex, nous observons une utilisation plus étendue de faux courtiers, de même que les manipulations techniques des plateformes de trading, ce qui n'a pas été particulièrement souligné par la littérature et les sources ouvertes lors de fraudes de cryptomonnaies. Alors que les services d'un courtier réglementé sont obligatoires pour les investissements Forex dans certains pays tel que le Canada, les investissements de cryptomonnaies peuvent se faire par quiconque (CSA, s.d). Cela peut donc expliquer la raison pour laquelle les fraudes liées aux courtiers sont en plus grande prévalence au niveau du Forex. Dans la même optique, des stratagèmes tels que le ICO frauduleux en cryptomonnaies ne sont pas possibles sur le marché de devises puisque quiconque ne peut en créer de nouvelles. Ainsi, nous notons que les différences des modus operandi sont directement liés aux caractéristiques propres aux deux marchés et de leur fonctionnement.

Par ailleurs, bien que les modus operandi comprenant l'utilisation de robots Forex se présentent dans les deux marchés, la prévalence n'est pas la même. On dénote une ascension de ce genre de robot en Afrique du Sud pour prédire les tendances de cryptomonnaies, mais ne représente pas le même degré d'implication dans les arnaques de cryptomonnaies qui permettent la commission de plusieurs stratagèmes lors d'une même fraude (Zimwara, 2021).

PARTIE 4 : VICTIMOLOGIE ET PRÉVENTION

4.1 Profil des victimes

De manière générale, la fraude à l'investissement touche un bassin de victimes diversifiées en termes d'âges, de situation socio-économique, d'éducation, etc. (Lokanan, M.

2014). Afin d'obtenir une meilleure idée de l'investisseur vulnérable aux fraudes à l'investissement, l'ACCOVAM a mené une étude à partir de de données des décisions du Tribunal de réglementation des valeurs mobilières (Ibid.). Celle-ci rapporte que les individus les plus à risque dans la société serait toute personne désirant assurer son avenir financier dont la vulnérabilité serait facilement exploitable par la promesse de rendements élevés rapide tout en comportant de faibles risques (Lokanan et Liu, 2021; Lokanan, M., 2014 ; AMF, 2021). D'ailleurs, autant au niveau Forex que des cryptomonnaies, la faible éducation aux activités de trading et le désir de faire rapidement de gros gains sont des caractéristiques qui reviennent auprès des victimes (Finance Magnate 2022 ; Giambrone Law 2022; AMF, 2021).

De l'autre côté, l'étude de Mueller et Bois (2020) a analysé la corrélation entre l'âge et la susceptibilité à la fraude à l'investissement selon le rôle protecteur et l'intelligence émotionnelle. Cette double utilisation de mesures offre des résultats qui divergent de plusieurs études sur le sujet où les auteurs ont opté pour l'analyse à une seule mesure ou même type d'escroquerie précis restreignant les résultats au niveau de l'âge (Mueller et Bois, 2020). Par exemple, les personnes âgées peuvent être plus susceptibles à des arnaques par téléphone, alors que les jeunes par messages sur les réseaux sociaux, tous deux reliés à des fraudes à l'investissement (Mueller et Bois, 2020 ; AMF, 2021.)

En ce sens, les résultats des différentes études peuvent varier en fonction de la façon dont les stratagèmes sont analysés. Par exemple, Lokanan et Liu (2021) rapportent que les investisseurs âgés de 60 ans et les retraités seraient plus susceptibles d'être victime de fraude à l'investissement. De l'autre côté, un rapport de la Federal Trade Commission rapporte que les individus dans la tranche d'âge de 20 à 49 ans auraient trois fois plus de de chance d'être victime d'arnaque par cryptomonnaie, dont ceux dans la trentaine serait le plus victimisé (Coin, L.J., 2022). Dans la même optique, AMF France soutient que la victimisation des individus plus jeunes est en augmentation dû à cette utilisation accrue du web moins utilisée chez les gens plus âgés (Ibid).

4.2 La recherche de victimes

Autant au niveau Forex que crypto, les criminels puisent généralement leur bassin de victimes par l'entremise de véhicules technologiques. D'une part, certains fraudeurs vont utiliser l'empoisonnement ou l'optimisation de moteurs de recherches (SEO) (Malinga, 2020; Which, 2022). En ce sens, lorsqu'un individu fera une recherche sur des moteurs tels que Google tapant des mots clés populaires comme investissement Forex ou crypto, les sites frauduleux apparaîtront automatiquement dans les premier résultats (Malinga, 2020.). Par la suite, les fraudeurs utilisent le marketing de masse en générant des publicités dans les journaux, la radio, la télévision ou plus fréquemment des sites internet ou même par courriel textos et appels afin d'attirer les victimes à consulter leurs plateformes frauduleuses (Autorité canadiennes en valeurs mobilières, s.d ; Which 2022). Ils peuvent accéder aux informations de contacts de milliers d'individus par des précédents vols d'informations par le moyen d'hameçonnage, ou simplement par les données personnelles en ligne dont les gens publient sur leurs réseaux (Steinberg, 2020). D'ailleurs, l'un des appâts qui attirent les individus plus jeunes sont la promotion de l'investissement Forex et crypto sur les médias sociaux ou les forums en ligne tel que Reddit afin de cibler des futur investisseurs se posant des questions ou démontrant en leur promettant des rendements élevés (Sasktoday, 2020). D'autres vont se créer des profils sur les réseaux sociaux ou de rencontre afin d'établir une relation avec un individu pour éventuellement l'attirer à faire des investissements frauduleux (CFTC, s.d).

4.3 Les conséquences des fraudes sur les marchés des Forex et de la cryptomonnaie

Un rapport du UK's regulatory framework for financial services rapporte que la portée des impacts chez les victimes de criminalité économique est considérable et ne se limite pas à la perte financière (Venkataramakrishnan, 2022). En effet, les expériences de fraudes vécues par les victimes causent des effets négatifs dans plusieurs sphères de leur vie : financier, social, émotionnel, etc. (Ibid.). Ces derniers se manifestent entres autres par la stigmatisation, la dépression, l'anxiété, le suicide et le retrait social (Ibid.). La problématique n'a donc pas seulement une conséquence financière, elle a un impact auprès des victimes sur leur santé psychologique et également leur qualité de vie.

4.4 Mesures de préventions

Tant que les marchés du Forex et de la cryptomonnaie seront actifs, les fraudes ne cesseront de se proliférer. Puisque nous ne pouvons éradiquer la problématique, nous devons nous consacrer sur des stratégies permettant de réduire considérablement la prévalence de ces fraudes à l'investissement. Nous nous sommes donc basées sur la "Protection Motivation Theory (PMT)" de Rogers (1975), modèle théorique utilisé en prévention de la cybercriminalité afin d'émettre nos recommandations. Ce dernier mise sur la proactivité de cibles potentielles afin de stimuler l'auto-protection (Doane et al., 2016). Doane et al. (2016) le définit comme suit :

« *L'adoption de mesures de protection par un individu dépend de sa perception de la menace (sévérité perçue et susceptibilité perçue) et de sa capacité à s'y adapter et à y faire face (efficacité de la réponse et auto-efficacité). Ces deux processus cognitifs seraient stimulés en présence d'une menace, ce qui déclencherait des comportements protecteurs dans le but d'en réduire les effets.*

La littérature portant sur les campagnes de prévention en cybersécurité avance plusieurs pistes intéressantes concernant les cybercrimes tel que l'amélioration de la visibilité, de même que l'intensification de ce que l'auteur appelle "messages préventifs" (Coutu, 2019). Étant donné que les fraudes étudiées sont de plus en plus perpétrées via des véhicules technologiques, nous sommes d'avis qu'une stratégie de maximisation de la visibilité des campagnes de prévention serait d'utilité en se concentrant sur les réseaux sociaux populaires tel qu'Instagram, Tiktok, Facebook, etc. sous formes de présentation accrocheuses. Coutu (2019) précise également de diversifier les campagnes sur différents canaux, ce dont nous appuyons étant donné que les fraudes ciblent un bassin diversifié d'investisseurs. De même, nous soutenons que les différentes campagnes doivent être adaptées à certains groupes cibles préalablement établis afin que le message y soit clair et compris de tous, tout en prenant le soin d'exposer explicitement les risques (Coutu, 2019) liés aux fraudes Forex et cryptomonnaie tel que par de réels témoignages, conséquences dévastatrices etc. . De cette façon, les menaces seront perçues commes réelles et susceptibles de se produire. Or, comme mentionné par O'Donnell (2019), nous devons être prudent à ne pas exagérer la visibilité des dites campagnes afin de ne pas créer un l'effet de

“*security fatigue*” où les gens se sentent submergés par la panoplie de menaces dont ils font face et se sentent donc impuissants (Ibid.).

Au niveau de la capacité à faire face aux risques et à s’y adapter, l’éducation financière est un moyen de prévention primordial en termes de fraudes à l’investissement (Lokanan, 2014). Comme mentionné plus haut, les marchés de cryptomonnaies et Forex comportent plusieurs technicalités dont les connaissances sont nécessaires afin de ne pas perdre son argent, de même que de se faire arnaquer par des individus malveillants. Singh et Misra (2022) proposent des programmes d’éducation financière incluant des signaux d’alertes afin de détecter les différents stratagèmes de fraude à l’investissement, de même que des caractéristiques émanant d'investissements légitimes. De cette façon, les nouveaux investisseurs ou moins expérimentés pourraient être en mesure de faire la différence entre de faux et véritables services (Singh et Misra, 2022).

Visant le même objectif, l’étude de Norris, Brookes et Dowell (2019) sur la psychologie de la victimisation des fraudes sur internet rapporte que la connaissances des stratagèmes consiste en un moyen de résilience. En ce sens, des forums, groupes ou plateformes de signalement de cyberfraudes peut être un moyen de prévention efficace afin de conscientiser les citoyens à de potentielles fraudes auxquelles ils pourraient être exposés. Par exemple, la clinique de cyber-criminologie de l’université de Montréal a lancé la plateforme communautaire Fraude-Alerte.ca qui permet aux citoyens de signaler les fraudes rencontrés sur internet (Clinique de cyber-criminologie, s.d). Les internautes peuvent donc être avertis des cyberfraudes en circulation et ce, en temps réel, de même que de s’entraider afin d’éviter de tomber dans les pièges (Ibid.). Ce genre de plateforme permet non seulement de jouer sur la perception de la menace, mais également de l’auto-efficacité des réponses.

D’autres moyens de prévention sous forme d’outil pourraient être utilisés par les citoyens tel que des vérificateurs de légitimité de plateformes. Par exemple, l’outil ScamDoc fait l’évaluation de confiance d’une identité numérique (site internet, plateforme en ligne, adresse courriel, etc.) (ScamDoc, s.d). Ce dernier offre un rapport sur plusieurs éléments tels que le nom de domaine, le trafic , les avis afin d’offrir un portrait de la légitimité du site (ScamDoc, s.d). Cet outil pourrait non seulement être utilisé tel que, mais un dérivé spécifique aux fraudes à

l'investissement pourrait être développé afin d'offrir des informations supplémentaires et renforcer l'évitement de plateformes frauduleuses, moyen de s'adapter aux risques en incluant les vérifications dans des réflexes sécuritaires. D'ailleurs, l'AMF québécois met à la disposition d'une liste des plateformes frauduleuses à jour, ce qui peut être une bonne ressource à consulter pour les investisseurs et qui devrait être davantage mise de l'avant sur l'arène public.

Finalement, une initiative gouvernementale visant à encourager les personnes découvrant des plateformes pourrait être instaurée. Cette dénonciation pourrait faire lieu d'une récompense monétaire et ainsi encourager un maximum d'individus à dénoncer ce genre de crime. Ceci permettrait d'appliquer un moyen de détection de façon interne au sein de la population et encouragerait par le fait même à la population à s'informer sur le sujet afin de trouver ce genre de plateforme. Cela pourrait même potentiellement engendrer une forme de dissuasion auprès des fraudeurs. D'ailleurs, en faisant un rapport des individus arrêtés face à ces dénonciations, les citoyens pourraient renforcer leur sentiment de contrôle sur la situation.

CONCLUSION

Les fraudes à l'investissement sont des crimes économiques omniprésents dans la société. La volatilité du marché des devises a ouvert la porte à de nombreux investisseurs à la recherche de gains, mais aussi à de nombreux fraudeurs qui tentent d'exploiter les vulnérabilités du marché et des investisseurs. Au fil du temps, l'engouement s'est dirigé vers l'investissement en cryptomonnaies, où le même phénomène est observable : les investisseurs ont été suivis de criminels tentant de dérober leurs économies. Nous avons relevé que les fraudes liées aux deux marchés étudiés relèvent d'utilisation de plateformes frauduleuses, les ventes pyramidales, les fraudes amoureuses et les fraudes reliés au remboursement. Les fraudeurs misent principalement sur la confiance et le déficit de connaissances requises afin de faire des investissements sur les marchés. Du côté des différences, le Forex fait place à plus de fraudes reliées à des manipulations techniques de courtiers en devises, ce qu'on ne retrouve pas dans les modus operandi des fraudes de crypto-monnaies. De plus, on dénote que les robots frauduleux ne sont pas aussi utilisés dans les arnaques de cryptomonnaies, comparativement à celles du Forex.

Au niveau de la victimologie, la recherche souligne qu'il n'y a pas spécifiquement de profil de l'investisseur victimisé type, mais qu'un désir d'assurer son avenir financier et des faibles connaissances techniques du marché son associé à une victimisation. D'ailleurs, Mueller et Bois, (2020) rapporte que les différentes caractéristiques sociodémographiques peuvent être interprétées différemment par la façon dont les fraudes sont étudiées, de même qu'elles peuvent varier en fonction des différents modus operandi liés aux différents stratagèmes de fraudes sur les marchés. Au niveau des secteurs, les fraudeurs attirent les potentielles victimes par l'entremise de différents véhicules technologiques : marketing de masse par courriel, texto, réseaux sociaux, empoisonnement des moteurs de recherche, applications de rencontre, etc. Malheureusement, les conséquences sur les victimes sont dévastatrices et ne touchent pas seulement le côté monétaire, mais aussi psychologique tel que la dépression, l'anxiété et le suicide.

Finalement, afin de lutter contre la problématique des fraudes sur le marché du forex et des cryptomonnaies, nous devons nous pencher sur une approche variée combinant plusieurs mesures de prévention. Nous nous sommes penchées sur la protection motivation theory de Rogers (1975) axé sur la proactivité des victimes afin de réfléchir à des moyens de prévention. D'une part, l'éducation financière est primordiale afin que les futurs et actuels investisseurs aient les connaissances adéquates pour mener des activités de trading et éviter des tentatives de fraudes. Ensuite, les plateformes communautaires et les outils de vérification de légitimité de site web sont primordiaux pour avertir les citoyens des différentes fraudes à l'investissement en circulation. De l'autre côté, un programme de dénonciation des fraudes à l'investissement pécuniairement récompensé pourrait être une solution permettant aux citoyens d'éviter les pertes bancaires. Pour finir, à l'ère de la technologie, la sensibilisation sur les réseaux sociaux pourrait être particulièrement efficace afin de rejoindre le plus de potentielles victimes et les empêcher d'être victime de fraude reliée au Forex et à la cryptomonnaie.

BIBLIOGRAPHIE

Admirals. (2022). Qu'est-ce que la volatilité en bourse et comment le trader ? *Admiral Market.* shorturl.at/ejwJY

Astrakhantseva, I., Astrakhantseva, R. & Los, A. (2021). Cryptocurrency fraud schemes analysis. *SHS Web of Conferences*, *106*, 02001. https://doi.org/10.1051/shsconf/202110602001

Autorité des marchés financiers. (2021). *Étude "arnaques à l'investissement".* AMF-France_Arnaques-a-linvestissement_202112_9f830412f1aefaaf54d3317eb7be64ad.pdf

Autorité des marchés financiers. (s.d). *La fraude à la Ponzi et la fraude pyramidale.* https://lautorite.qc.ca/grand-public/types-de-fraude/la-fraude-a-la-ponzi-et-la-vente-pyramidale

Autorité des marchés financiers. (2022). *Les fraudes liées aux crypto actifs.* https://lautorite.qc.ca/grand-public/types-de-fraude/fraudes-cryptos

Autorité des marchés financiers. (2022). *Marché des devises – FOREX C'est très risqué*. https://lautorite.qc.ca/grand-public/investissements/investisseurs-avertis/marche-des-devises-forex

Autorité des marchés financiers. (s.d). *Plateformes de négociation en ligne frauduleuses.* https://lautorite.qc.ca/grand-public/types-de-fraude/plateformes-de-negociation-en-ligne-frauduleuses

Avatrade. (s.d). *How to spot Forex scams.* Friedberg Direct. https://www.avatrade.ca/education/trading-for-beginners/forex-scams

Banque Nationale (2022). *Fraude à la cryptomonnaie : comment éviter les pièges*. https://www.bnc.ca/particuliers/conseils/securite/fraude-cryptomonnaie-eviter-les-pieges.html

Bélanger, M.F, Yates, J. et De Rosa, N. (2022). Tout perdre en quelques clics : des Canadiens victimes d'une fraude internationale. *Radio-Canada.* https://ici.radio-canada.ca/recit-numerique/3574/cryptomonnaie-canada-fraude-internationale

Berecz, C. (s.d). *Cryptocurrency Fraud: What to Know & How to Protect your Exchange*. Seon. https://seon.io/resources/how-to-protect-your-crypto-exchange-from-fraud/

Bloomberg. (2022). *Thai youtuber "Nutty" allegedly cheats Forex investors of B2bn.* Bangkok Post. https://www.bangkokpost.com/thailand/general/2380330/thai-youtuber-nutty-allegedly-cheats-forex-investors-of-b2bn

Boccadutri, C. (2021). *Italy: Fake Forex Lawyers: No Leniency For Scam Victims.* Mondaq. https://www.mondaq.com/italy/white-collar-crime-anti-corruption-fraud/1091332/fake-forex-lawyers-no-leniency-for-scam-victims-

Boccadutri, C. (2020). *How to recognize a forex scam.* Boccadutri International Law Firm. *https://www.boccadutri.com/how-to-recognize-a-forex-scam/*

Canadian Securities Administrators. (s.d). *Forex Scams.* *https://www.securities-administrators.ca/investor-tools/avoiding-fraud/common-frauds-and-scams/#forex-scam*

CFI. (2022). *Interbank Market*. https://corporatefinanceinstitute.com/resources/economics/interbank-market/

Clinique de cyber-criminologie. (s.d). *Nos services : Fraude-Alerte.ca.* https://www.clinique-cybercriminologie.ca/services

Coin, L. J. (2022). Cryptomonnaie : 1 milliard de $ volés sur les réseaux sociaux – Un bilan dévoilé par les États-Unis. *Journal du Coin.* https://journalducoin.com/actualites/1-milliard-dollars-voles-reseaux-sociaux-bilan-etats-unis/

Commodity Futures Trading Commission. (s.d). *Customer Advisory: Avoid Forex, Precious Metals, and Digital Asset Romance Scams.* https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/CustomerAdvisory_RomanceScam.html

Coutu, C. (2019). *La prévention de la cybercriminalité : résultats d'une enquête sur les effets perçus d'une campagne de prévention réalisée par une institution financière* [mémoire de maîtrise, Université de Montréal]. Papyrus. https://papyrus.bib.umontreal.ca/xmlui/handle/1866/23715

Daniels, N. (2022). *Crypto Pump and Dump Scams Explained – How to Avoid Them*. VPNoverview.com. https://vpnoverview.com/privacy/finance/crypto-pump-and-dump/

Delage, V. Brandlhuber, C., Tuyls, K. et Weiss, G. (2011). Multi-Agent based simulation of FOREX exchange market [Maastricht University]. *ResearchGate.* https://www.researchgate.net/publication/266874598_MultiAgent_based_simulation_of_FOREX_exchange_market

Drake, T. (2021). *What You Need to Know to Get Started in Forex Trading in Canada.* Maplemoney. https://maplemoney.com/forex-trading/

Doane, A. N., Boothe, L. G., Pearson, M. R. et Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computers in Human Behavior* (60), 508-513. https://doi.org/10.1016/j.chb.2016.02.010

Finance Magnates. (2020). A Rural Manitoba Man Loses $ 550K to Forex Fraud. F*inancial and Business News.*

https://www.financemagnates.com/forex/brokers/a-rural-canadian-man-loses-550k-to-offshore-forex-fraud/

FXCM Research Team. (2018). *What is Front-running ?* https://www.fxcm.com/ca/insights/what-is-front-running/

Giambrone. (s.d). *Forex Lawyers-Forex Trading Scams.* https://www.giambronelaw.com/site/servicesforindividuals/forex-litigation-lawyers/forex-trading-scams/

HEC. (2022). *Marketing par affiliation pour les débutants 2022.* https://digital.hec.ca/blog/marketing-par-affiliation-2022/

Hope, A. (2022). *Everything You Need to Know About the Types of Forex Scams and How to Avoid Them.* Researchsnipers. https://researchsnipers.com/everything-you-need-to-know-about-the-types-of-forex-scams-and-how-to-avoid-them/

IG. (s.d). *What is forex and how does it work?* https://www.ig.com/en/forex/what-is-forex-and-how-does-it-work

Jackson, A-L., Curry, B. (2022). A basic guide to forex trading. *Forbes.* https://www.forbes.com/advisor/investing/what-is-forex-trading/

Jendruszak, B. (2022). *Forex Fraud : How to Detect It & Avoid Different Scam Methods.* Seon. https://seon.io/resources/forex-fraud/

Kumar, R. (2014). Stock Markets, Derivatives Markets, and Foreign Exchange Markets. *Strategies of Banks and Other Financial Institutions: theories and cases, (5)* 125-164. https://doi.org/10.1016/B978-0-12-416997-5.00005-1

Lacey, D., Goode, S., Pawada, J. and Gibson, D. (2020), The application of scam compliance models to investment fraud offending, *Journal of Criminological Research, Policy and Practice*, 6 (1), 65-81. https://doi.org/10.1108/JCRPP-12-2019-0073

Leblanc, M. (2022). Fraude : 275 M $ de perte financière au Canada en 2021. *Radio-Canada.* https://ici.radio-canada.ca/nouvelle/1870131/arnaque-investissement-vol-finance-banque-fraude-canada

Li, S. (2016). The Currency Exchange Market in East Asia. *East Asian Business in the New World : Helping Old Economies Revitalize*, (7), 95-102. https://doi.org/10.1016/B978-0-08-101283-3.00007-5

Lokanan, E. N. (2014). The demographic profile of victims of investment fraud: A Canadian perspective. *Journal of Financial Crime*. 21(2), 226-242.

http://dx.doi.org/10.1108/JFC-02-2013-0004l

Lokanan, E. N., Liu, S. (2020).The demographic profile of victims of investment fraud: an update. *Journal of Financial Crime*, 28(3), 647-658.

http://dx.doi.org/10.1108/JFC-09-2020-0191

Malinga, S. (2020). More consumers fall prey to forex trading scams in SA. *Itweb.* https://www.itweb.co.za/content/KPNG8v8KEZBq4mwD

Market Business News. (s.d). *What is Forex?* Financial Glossary. https://marketbusinessnews.com/financial-glossary/forex/

Masama, B. (2021). Factors Influencing the Trading Results of Forex and Crypto Traders in Africa. *Working paper MC/2021/005.* http://dx.doi.org/10.2139/ssrn.3957785

Melvin, M., Norrbin, S. (2017). The Foreign Exchange Market. *International money and finance*, 9 (7), 3-24. https://doi.org/10.1016/B978-0-12-804106-2.00001-0

Mueller, A.E., Wood, A.S., Hanoch, Y., Huang, Y. et Reed, L.C. (2020). Older and wiser: age differences in susceptibility to investment fraud: the protective role of emotional intelligence. *Journal of Elder Abuse & Neglect*, 32(2), 152-172. https://doi.org/10.1080/08946566.2020.1736704

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimization: A systematic review. *Journal of Police and Criminal Psychology*, 34(3), 231-245. https://doi.org/10.1007/s11896-019-09334-5.

O'Donnell, A. (2019). Create an effective security awareness training program. Lifeware.

Paxful. (2020). Le trading de crypto monnaie est-il plus rentable que le trading Forex ? *Paxful.* https://paxful.com/university/fr/trading-forex-ou-crypto/?fbclid=IwAR0rfa_peSdzESkyQ23z4EAjw8yPrd1_KwMJBp_IPc30WdtHtCM_fe8r-4A

Revenu Québec. (s.d). *Monnaie virtuelle et cryptomonnaies*. https://www.revenuquebec.ca/fr/une-mission-des-actions/vous-aider-a-vous-conformer/quest-ce-que-leconomie-numerique/monnaie-virtuelle/

ScamDoc (s.d). *ScamDoc : évaluation de confiance numérique.* https://fr.scamdoc.com/

Staszkiewicz, P., Staszkiewicz, L. (2015). Introduction to Finance and Financial Markets. *Finance : A Quantitative Introduction*, 1 (1), 1-17. https://doi.org/10.1016/B978-0-12-801584-1.00001-9

Singh, N. K., Misra, G. (2022). Victimization of investors from fraudulent investment schemes and their protection through financial education. *Journal of Financial Crime, 1359-0790.* http://dx.doi.org/10.1108/JFC-07-2022-0167

South Florida Caribbean News. (2022). What Are The Types of Forex Scams, and How Can You Protect Your Account? *South Florida Caribbean News.* https://sflcn.com/types-of-forex-scams-and-how-can-you-protect-your-account/

Steinberg, S. (2020). The latest ways identity thieves are targeting you — and what to do if you are a victim. *CNBC.* https://www.cnbc.com/2020/02/27/these-are-the-latest-ways-identity-thieves-are-targeting-you.html

TD Ameritrade. (2018). *Investing Basics: Forex.* https://www.youtube.com/watch?v=_tEbIzKbZhY&t=85s

TD Ameritrade. (2020). *What Are currency pairs?* https://www.youtube.com/watch?v=b0PpzEuCc9A

Trading view. (s.d). *Markets: Forex Market.* https://www.tradingview.com/markets/currencies/

Ucchino, P. (2022). *Is Forex trading legal in Canada.* Investingoal. https://investingoal.com/is-forex-trading-legal-canada/

Ucchino, P. (2022). *10 Worst Trading Scams and How to Avoid Them*. Investingoal. *https://investingoal.com/types-of-trading-scams/*

Venkataramakrishnan, S. (2022). Victims of financial crime suffer psychological shocks. *Financial Times.* *https://www.ft.com/content/12b2dbe7-9810-48cb-932f-207e6aefcf00*

Watkins, G. (2018). *The #1 Problem of Forex Affiliates: Not Getting Paid*. Valutrades. https://www.valutrades.com/en/blog/affiliate/the-1-problem-of-forex-affiliates-not-getting-paid

Which (2022). One in five fraud victims send money to criminals via cryptocurrency. *Which.*

https://www.which.co.uk/news/article/one-in-five-fraud-victims-send-money-to-criminals-via-cryptocurrency-alCPq3K8KPa8

Zimwara, T. (2021). The Rise of Fake Crypto Trading Bots : Steps Users Must Take to Avoid Getting Scammed. *Bitcoin News*. https://news.bitcoin.com/rise-of-fake-crypto-trading-bots-steps-users-must-take-to-avoid-getting-scammed/?fbclid=IwAR1zhbJR7MsAnACiyo_pZ_s7P-Yeag4WWzDQ1ygTIsFdOxfirI7xnEE65UA