THOMSON REUTERS
ACCELUS™

TECHNOLOGIES UTILISÉES POUR LUTTER CONTRE LE BLANCHIMENT D'ARGENT DANS LA NOUVELLE ÈRE DES DEVISES NUMÉRIQUES

Déclaration d'intention

Drogue, prostitution, jeux illégaux, fraude, extorsion : partout où de l'argent est en relation avec une activité criminelle, il y a un escroc qui veut « blanchir » ou légitimer cet argent pour qu'il puisse circuler dans le système financier mondial, sans que l'on se pose de questions.

À l'image d'un grand nombre d'activités illégales, le blanchiment d'argent fait l'objet d'une révolution, en quelque sorte. C'est parce que la technologie, que ce soient les casinos en ligne et les sites Internet de médias sociaux ou l'apparition de devises numériques, fournit aux criminels d'autres moyens de blanchir leurs bénéfices illégaux. Malgré des réglementations importantes destinées à empêcher le blanchiment d'argent dans les systèmes financiers américains et instituées peu de temps après les tragiques événements du 11 septembre 2001, les organismes d'application de la loi et les institutions financières continuent à tout mettre en œuvre pour garder une longueur d'avance sur les criminels.

Ce livre blanc, proposé par Thomson Reuters, étudie les changements qui s'opèrent dans les activités de blanchiment d'argent illégales, mais aussi ce que font les institutions financières et les organismes d'application de la loi pour lutter contre cette menace croissante pour la stabilité du système financier mondial, par l'intermédiaire de nouvelles stratégies, réglementations et technologies.

THOMSON REUTERS™

ONT CONTRIBUÉ À CET OUVRAGE

Cindy Williamson
CFE, CAMS, Enforcement Analyst III, National White Collar Crime Center (nw3c.org)

Jason Vazquez
Senior Vice President and BSA/AML Compliance Officer, Provident Bank (providentbanking.com)

Jason Thomas
Senior Strategic Analyst, Thomson Reuters

Katherine Sagona-Stophel
Government Analyst, Thomson Reuters

TABLE DES MATIÈRES

DÉFINITION DU PROBLÈME

Le 28 mai 2013, des procureurs américains mirent en examen sept personnes impliquées dans une opération de cybercrime mettant en cause une banque en ligne qui aurait géré plus de 6 milliards de dollars pour des trafiquants de drogue, des pornographes juvéniles, des usurpateurs d'identité, des pirates informatiques et d'autres criminels, tous connectés via l'échange anonyme de devises numériques. Selon les autorités américaines, ce fut la plus grosse affaire de blanchiment d'argent de l'histoire américaine.

Au centre de cette soi-disant opération de blanchiment de cyberargent se trouve Liberty Reserve, une société de transfert de devises et de traitement de paiements basée au Costa Rica. Selon Reuters, Liberty Reserve a traité environ 12 millions de transactions par an depuis 2006. La société permettait aux titulaires de compte de créer des comptes anonymes et de convertir de l'argent réel en devises numériques anonymes et intraçables appelées LR.

L'affaire Liberty Reserve représente un changement notable dans la lutte contre le blanchiment d'argent, à savoir le processus qui consiste à transformer de l'argent et des capitaux acquis par des voies illégales en argent légal (blanchi). Le blanchiment d'argent est souvent un processus secondaire, précédé par une activité illégale, comme le trafic de drogue ou une escroquerie en ligne. Dans certains cas, le blanchiment d'argent peut être utilisé par des organisations terroristes pour menacer et/ou mener des attentats basés sur des idées philosophiques. L'un des éléments clés de ce processus consiste à garder l'anonymat et à éviter toute transparence en cours de route. Alors que les blanchisseurs se limitaient autrefois aux devises physiques, l'arrivée des devises numériques augmente la complexité de la lutte mondiale contre cette activité.

La Financial Action Task Force (FATF), une organisation intergouvernementale regroupant 36 pays, estime que le blanchiment d'argent représente de 2 à 5 pour cent du produit intérieur brut (PIB) annuel mondial, ce qui équivaut à un montant estimé de 1,38 à 3,45 billions de dollars. Mais comme ce problème est très répandu, la FATF précise qu'il n'est pas possible d'estimer la somme d'argent réellement blanchie à travers des systèmes financiers légaux et illégaux de par le monde.

« Le blanchiment d'argent et le financement du terrorisme sont des crimes financiers aux effets économiques », a déclaré Min Zhu, directeur général adjoint du Fonds Monétaire International (FMI) dans une alerte du FMI de 2013. « Ils (les blanchisseurs) peuvent menacer la stabilité du secteur financier d'un pays ou sa stabilité extérieure, plus généralement. Il est essentiel de lutter efficacement contre le blanchiment d'argent et le financement de régimes terroristes pour protéger l'intégrité des marchés et du cadre financier mondial car ces mesures permettent d'atténuer les facteurs qui facilitent les abus financiers. Le fait d'empêcher et de lutter contre le blanchiment d'argent et le financement du terrorisme répond non seulement à un impératif moral, mais aussi à un besoin économique. »

La lutte contre le blanchiment d'argent est devenue d'autant plus urgente après les tragiques événements aux États-Unis le 11 septembre 2001 (9/11). Le gouvernement américain, le FMI et d'autres institutions gouvernementales du monde entier ont intensifié leurs efforts contre le blanchiment d'argent une fois qu'il est devenu évident que l'organisation terroriste Al-Qaïda avait utilisé des techniques de blanchiment d'argent pour financer avec succès les attentats du 11 septembre. Selon une enquête de PBS Frontline, il apparaît que l'argent collecté par des associations islamiques en Europe et aux États-Unis a été blanchi par le système bancaire européen pour organiser les attentats du 11 septembre et d'autres opérations terroristes.

« Il est essentiel de lutter efficacement contre le blanchiment d'argent et le financement de régimes terroristes pour protéger l'intégrité des marchés et du cadre financier mondial. »

Aujourd'hui, plus de 10 ans après le 11 septembre, le problème du blanchiment d'argent est d'autant plus urgent du fait qu'il peut déstabiliser la santé financière des pays. Le blanchiment d'argent s'est développé dans des pays dont les contrôles financiers sont inefficaces ou délibérément laxistes, ce qui a permis au crime organisé et/ou aux groupes terroristes de déplacer des fonds facilement sans être détectés. Le problème, comme certains gouvernements tels que l'Allemagne l'ont exprimé publiquement à propos de la stabilité financière de Chypre (dans le cadre des luttes financières de l'Union européenne), c'est

l'impact de type cancérigène que le blanchiment d'argent peut avoir sur des systèmes financiers plus importants.

Le problème croissant du blanchiment d'argent a poussé le ministère des Finances américain à annoncer en novembre 2012 la formation d'un nouveau détachement spécial anti-blanchiment d'argent, selon un communiqué Reuters de Brett Wolff (12 novembre 2012). David Cohen, le sous-secrétaire des renseignements sur la finance et le terrorisme du ministère des Finances américain, a déclaré que le détachement spécial a été formé prioritairement à cause du « changement extraordinaire » qui a lieu dans le secteur financier, dû aux innovations technologiques et financières.

« Les procédés de blanchiment d'argent eux-mêmes deviennent aussi de plus en plus sophistiqués et internationaux », a déclaré Cohen dans le rapport Reuters. « Les progrès spectaculaires en matière de technologie et de finance ont eu comme effet secondaire d'amplifier le risque potentiel de blanchiment d'argent. »

Selon un échantillonnage d'enquêtes documentées et menées à leur terme, rassemblées par l'Internal Revenue Service (IRS) pour les années 2010 et 2011, de l'argent est blanchi régulièrement tous les jours aux États-Unis, que ce soit dans de grandes métropoles ou dans de petites villes du centre de l'Amérique. Voici des exemples de blanchiment d'argent :

- Le 14 mai 2013, le département de la Sécurité intérieure des États-Unis a cité à comparaître Dwolla, un service de paiement par téléphone mobile connu, leur demandant de cesser toute activité utilisant la devise numérique Bitcoin de Mt. Gox (mtgox.com), citant le fait que Mt. Gox et sa filiale, Mutum Sigillum LLC, une société Delaware, n'étaient pas autorisées à transférer de l'argent.
- *Gambling News* (10 avril 2013) a rapporté la mise en examen de 34 personnes et 23 sociétés en relation avec Legendz Sports (alias Legands Sports), un opérateur de paris sur le sport en ligne accusé de « racket, blanchiment d'argent et jeu illégal ».
- Le 1er août 2012, la division de Los Angeles du FBI a annoncé que des juges américains et australiens, voulant récupérer plus de 24 millions de dollars en capitaux, ont cité à comparaître e-Bullion.com, que la partie plaignante accusait de transférer de l'argent illégalement. « Par l'intermédiaire du site e-Bullion.com, les gens ouvraient des comptes avec de l'argent réel, qu'ils utilisaient pour acheter des devises électroniques virtuelles. Le FBI affirme que e-Bullion permettait aux gens de frauder pour transférer de l'argent dans le monde entier tout en restant virtuellement anonymes et en évitant un grand nombre d'obligations bancaires au niveau international. »
- Le 26 août 2011, Joy Edison, résidant à Elkton, dans le Maryland, fut condamné à 70 mois de prison pour avoir contribué à blanchir plus de 400 000 $ de recettes provenant de la drogue. En sept ans, Edison et un groupe de complices ont blanchi les recettes émanant de ventes d'héroïne dans des casinos de Las Vegas, des billets de loterie du Maryland, une entreprise de voitures d'occasion et des biens achetés par Edison via une société-écran, J. Edison Properties.
- En juillet 2006, Arthur Budovsky et Vladimir Kats ont été mis en examen par l'État de New York parce qu'ils géraient une société de transfert d'argent illégal, GoldAge, Inc., dans leurs appartements de Brooklyn. Les accusés ont transféré au moins 30 millions de dollars vers des comptes de devises numériques du monde entier. Source : National Drug Intelligence Center, juin 2008.
- Hector Dominguez-Gabriel, trafiquant de drogue et blanchisseur d'argent international basé au Mexique, a été condamné à 240 mois de prison le 12 août 2011 pour importation de drogue et blanchiment d'argent. Dominguez-Gabriel a blanchi des millions de dollars de recettes provenant de la drogue au Mexique en faisant systématiquement de petits dépôts structurés sur des comptes bancaires dans tous les États-Unis.
- Reuters a rapporté que le FBI menait une enquête dans les casinos virtuels de Second Life en avril 2007 concernant la possibilité d'une activité illégale d'après l'Illegal Gambling Business Act de 1970 (loi relative à la pratique de jeux illégaux) ou l'Unlawful Internet Gambling Enforcement Act (loi contre la pratique de jeux illégaux sur Internet). Dans son *National Gang Threat Assessment: Emerging Trends de 2011*, le National Gang Intelligence Center a noté la possibilité que Second Life soit une source permettant aux criminels de commettre une large gamme d'activités illégales.

- Selon le *FBI Intelligence Assessment* (24 avril 2012), « les groupes du crime organisé (à partir de juin 2011) utilisaient un jeu de rôles en ligne pour faciliter le blanchiment d'argent en achetant des devises virtuelles avec les recettes de l'activité criminelle. Les devises virtuelles étaient utilisées pour acheter des articles virtuels du jeu qui étaient ensuite vendus à d'autres joueurs contre de l'argent blanchi. »

Dans sa forme la plus simple, le blanchiment d'argent est un procédé, selon une monographie de la Rand Corporation, *Cyber Payments and Money Laundering,* qui existe uniquement parce que l'argent, c'est-à-dire les billets et les pièces, est trop encombrant et lourd à transporter en grandes quantités, ce qui rend difficile son déplacement d'une personne ou d'une organisation à une autre, d'un État à l'autre ou d'un pays à l'autre.

Indépendamment des institutions financières américaines, voici d'autres structures financières utilisées fréquemment par les blanchisseurs :

- Des comptes bancaires à l'étranger et offshore situés dans des pays qui ont des lois de non divulgation protégeant l'identité des individus ou des sociétés qui ouvrent des comptes dans leur pays.
- Des sociétés-écrans utilisées pour canaliser l'argent via des activités « légitimes ».
- Des systèmes bancaires parallèles ou souterrains, qui existent dans des pays tels que l'Inde, le Pakistan, la Chine et d'autres parties de l'Asie, et qui sont gérés par des groupes du crime organisé ou des alliances de gangs.
- Le blanchiment d'argent commercial (Trade-based money laundering ou TBML), à savoir le blanchiment de fonds à travers le commerce de biens et services. En 2006, la FATF a remarqué l'utilisation croissante du TBML par les organisations criminelles et les groupes terroristes, tandis que différents gouvernements à travers le monde renforcent les règles et réglementations relatives au blanchiment d'argent. Cependant, le TBML reste un aspect négligé du blanchiment d'argent à ce jour.
- Les cartes prépayées, souvent appelées cartes-cadeaux, et facilement disponibles dans le pays dans les stations-service, les chaînes de drugstores et les détaillants à prix réduit, sont devenues si appréciées par les blanchisseurs que le Financial Crimes Enforcement Network (FinCEN) (réseau d'application de la loi contre les crimes financiers), une section du ministère des Finances américain, étudie de nouvelles réglementations qui obligeraient les voyageurs à déclarer les cartes prépayées d'un montant supérieur à 10 000 $ à la douane, selon le magazine Personal Finance Digest (4 avril 2013).

blanchiment d'argent, travaillant pour le National White Collar Crime Center (NW3C) (Centre national des crimes économiques), croit que pour monter un dossier solide, il faut relier le blanchiment d'argent à une action illégale spécifique, telle que la fraude hypothécaire, le trafic de drogue ou la fraude par courriel. Les lois fédérales relatives au blanchiment d'argent sont multiples, mais les lois sur le blanchiment d'argent d'un État à l'autre sont incohérentes, explique Williamson.

« Les groupes criminels sont à la pointe de la technologie pour commettre leurs crimes et cacher les recettes de leurs activités. Par conséquent, il faut plus de stratégie dans l'application de la loi pour identifier les activités criminelles et réunir des renseignements et des preuves », a déclaré Williamson.

« Beaucoup d'organismes d'application de la loi sont préoccupés par les moyens technologiques alarmants que les criminels ont à portée de main. »

« Beaucoup d'organismes d'application de la loi sont préoccupés par les moyens technologiques alarmants que les criminels ont à portée de main », a-t-elle ajouté.

Selon Williamson, les crimes basés sur la technologie seraient en augmentation en partie parce que les criminels se sentent plus en sécurité.

« Pourquoi risquer de se faire tuer ou supporter une longue peine de prison pour trafic de drogue alors qu'on peut gagner de l'argent plus vite et avec moins de risques (les peines de prison pour les crimes économiques sont moins longues) en menant des activités telles que la fraude hypothécaire ou la fraude aux soins de santé ? », a déclaré Williamson. « Ainsi, les investissements technologiques permettent aux groupes criminels de blanchir l'argent plus vite et de façon plus sûre. »

Point essentiel : les criminels investissent dans la technologie pour blanchir l'argent. Les institutions financières et les organismes d'application de la loi doivent investir dans la technologie également.

LE BLANCHIMENT D'ARGENT A L'ÉPOQUE NUMÉRIQUE

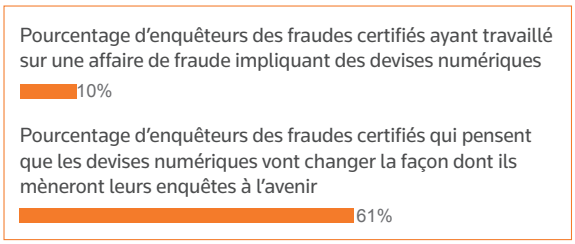
L'une des dernières tendances du blanchiment d'argent, ce sont les devises numériques. Beaucoup de gens commencent à peine à entendre parler de l'utilisation croissante des crypto-devises virtuelles indépendantes, telles que Bitcoins, Litecoins, Zen et Namecoins. Mais des devises en ligne et alternatives existent bien dans de nombreux endroits, des Linden Dollars utilisés dans le jeu en ligne Second Life aux Justice Points dans World of Warcraft, en passant par Berkshares, une devise alternative créée par cinq banques pour promouvoir le commerce dans la région du Berkshire, à l'ouest du Massachusetts. Et là où il y a des chances d'échanger de l'argent réel contre de l'argent virtuel, il y a une possibilité de blanchiment d'argent.

Certaines devises virtuelles sont totalement anonymes, contrairement aux transactions par carte de crédit ou chèque nominatif, qu'on peut relier à une personne ou une entité particulière. Les devises virtuelles ne sont pas comme les dollars, les yen ou les euros car aucun organisme gouvernemental ou centralisé de réglementation ne réglemente leur valeur ou leur utilisation. Elles sont échangées librement et de façon anonyme sur des réseaux poste-à-poste dans le monde entier.

Comme certaines devises virtuelles peuvent être échangées librement sans être tracées, elles peuvent être utiles dans les profondeurs d'Internet, connues sous le nom de Web invisible, que les groupes du crime organisé, les cellules terroristes et autres entités obscures, des pornographes juvéniles aux trafiquants d'humains, considèrent comme leur territoire. En résumé, le Web invisible est la partie cachée du Web qui « ne peut pas être indexée par les moteurs de recherche – un endroit où Google ne se rend pas », notent les auteurs Pablo Albarracin et Christopher Holloway dans leur article sur le Web invisible du 17 décembre 2012 pour Worldcrunch.com. « Proposant anonymat et liberté, le Web invisible s'est transformé au fil des ans (certains disent qu'il représente 90 pour cent du contenu disponible sur Internet) en un grand entrepôt inhospitalier et peu exploré qui peut tout accueillir, du plus innocent au plus impitoyable et inimaginable. »

Même si la nature anonyme du Web invisible est un élément crucial pour les personnes qui se battent contre les régimes répressifs du monde entier, et pour les mouvements hacktivistes tels qu'Anonymous, le Web invisible est plutôt associé au trafic de drogue et d'armes, au terrorisme et à la pornographie juvénile. Par exemple, certains sites Internet sont devenus des détaillants en ligne pour les transactions illégales relatives à la drogue, aux armes illégales ou à la pornographie juvénile, permettant aux criminels d'utiliser des devises numériques comme moyen privilégié de paiement.

Les enquêteurs des fraudes sont préoccupés par les devises numériques



Source : Thomson Reuters – Enquête de l'ACFE, avril 2013

Pourtant, ce n'est pas la peine d'aller dans le monde souterrain du Web invisible pour accumuler des devises virtuelles. N'importe qui, de la ménagère de moins de 50 ans au dealer chevronné, peut acheter des devises virtuelles sur eBay ou Craigslist. Et c'est bien ce qui inquiète les organismes d'application de la loi.

À cause de l'intérêt grandissant qu'on leur porte, le FinCEN a annoncé de nouvelles réglementations anti-blanchiment d'argent concernant les devises virtuelles en mars 2013. Selon un rapport du Wall Street Journal écrit par Jeffrey Sparshott (21 mars 2013), « les sociétés qui délivrent ou échangent ces devises en ligne de plus en plus populaires seront désormais réglementées au même titre que les fournisseurs d'ordres de paiement traditionnels comme Western Union Co. Elles auront de nouvelles obligations comptables et devront obligatoirement rapporter les transactions de plus de 10 000 $. Cependant, les nouvelles réglementations ne s'appliquent pas aux individus qui n'utilisent les devises virtuelles que pour acheter des biens réels ou virtuels. »

Cela laisse de l'espace pour les mondes virtuels qui utilisent ou proposent des devises en ligne, ce qui permet aux jeux en ligne multi-joueurs de servir de canaux non réglementés pour les blanchisseurs, selon Jason Thomas, analyste stratégique senior chez Thomson Reuters.

« Le blanchiment d'argent par l'intermédiaire de ces énormes jeux en ligne multi-joueurs a longtemps été ignoré par les organismes d'application de la loi parce qu'il était perçu comme trop complexe », a remarqué Thomas. « Ces jeux en ligne, et le Web invisible en général, peuvent être très intimidants. Les sous-cultures étranges, mais aussi la taille de tout cet univers, peuvent paraître écrasantes. Avec des billions de transactions, beaucoup d'organismes d'application de la loi ne savent pas par où commencer. »

Tandis que la relation entre les devises numériques et le blanchiment d'argent ne fait qu'émerger, elle apparaît sur l'écran radar des organismes d'application de la loi et des établissements financiers.

Dans une enquête de la Thomson Reuters-Association of Certified Fraud Examiners (ACFE) (Association des enquêteurs des fraudes certifiés) en avril 2013, 10 pour cent d'entre eux déclarent avoir travaillé sur une affaire de fraude impliquant des devises numériques et 61 pour cent prévoient que la popularité croissante des devises numériques va changer la façon dont ils mèneront leurs enquêtes à l'avenir.

« Par ailleurs, certains organismes d'application de la loi envisagent avec circonspection le fait de travailler en présence de nouvelles technologies, craignant de créer par là même un précédent », a ajouté Thomas.

BLANCHIMENT D'ARGENT ET CONFORMITÉ

On s'attend à ce que le blanchiment d'argent se fasse dans les ténèbres de notre monde, comme le Web invisible, mais souvent, il peut se produire en pleine lumière, au sein même du système financier classique. Le 11 décembre 2012, HSBC Holdings Plc (HSBC), l'une des institutions financières les plus grandes au monde, a accepté de payer une amende d'un montant record de 1,92 milliard de dollars au ministère de la Justice américain, pour avoir permis le blanchiment de millions de dollars par les cartels de la drogue Sinaloa au Mexique et Norte del Valle en Colombie via les établissements bancaires mexicains et américains de la banque, selon Reuters (11 décembre 2012).

Selon Reuters, c'est la troisième fois en 10 ans qu'HSBC est pénalisée pour contrôles laxistes. « La conformité [à HSBC] était terriblement inadéquate », a remarqué Loretta Lynch, procureure générale à Brooklyn.

Thomas a déclaré qu'il est très difficile pour les établissements financiers de connaître leurs clients et de signaler des transactions qui paraissent suspectes. « La technologie existe par l'intermédiaire de fournisseurs tels que CLEAR et World-Check pour pouvoir identifier les criminels », a déclaré Thomas. « Et grâce à des technologies d'exploration des données complémentaires, nous pouvons prendre ces informations et faire le lien entre une personne suspecte et d'autres personnes susceptibles de participer à l'activité criminelle. »

Par ailleurs, a noté Thomas, « les établissements financiers possèdent la technologie pour identifier d'autres techniques de blanchiment de l'argent, comme l'ouverture d'un compte au nom d'une personne décédée. »

La solution pour contrôler une activité de blanchiment d'argent est de repérer les mouvements inhabituels dans le transfert de l'argent illégal vers le circuit d'argent légal. Le premier indice est souvent le changement de vitesse des flux de fonds entrants et sortants.

« Les meilleurs blanchisseurs comprennent le système. Ils sont patients. Ils déplacent l'argent dans les systèmes financiers internationaux lentement et en petites quantités moins suspectes », a déclaré Thomas. « Les blanchisseurs qui se font prendre sont impatients. Ils veulent déplacer de grandes quantités d'argent dans le système rapidement. »

La solution pour contrôler une activité de blanchiment d'argent est de repérer les mouvements inhabituels dans le transfert de l'argent illégal vers le circuit d'argent légal. Le premier indice est souvent le changement de vitesse des flux de fonds entrants et sortants.

« Le problème, c'est que plus nos souricières sont sophistiquées, plus les souris deviennent intelligentes », a remarqué Jason Vazquez, premier vice-président et déontologue BSA/AML de Provident Bank, une banque fondée il y a 120 ans, dont le siège social se situe à Montebello, dans l'État de New York, et qui gère plus de 3,7 milliards de dollars de capitaux.

Avant le 11 septembre, explique Vazquez, la plupart des banques américaines suivaient une liste générale d'activités pour se conformer au Bank Secrecy Act (BSA), un projet de loi devenu loi en 1970 qui a lancé un système de rapports pour les transactions financières supérieures à 10 000 $ - une étape significative pour contrôler le flux des recettes illégales. Même si la démarche était importante, le

programme du BSA n'était pas la priorité pour un grand nombre de banques ou d'examens menés par les organismes de réglementations des États ou fédéraux.

Mais le 11 septembre, suivi du USA Patriot Act, ont largement changé la donne, imposant des règles et réglementations plus strictes sur les établissements financiers afin de contrôler les transactions financières et les activités de blanchiment d'argent susceptibles de financer des activités terroristes.

« Le Patriot Act a mis la barre plus haut et a mis tout le monde, notamment les établissements financiers non dépositaires, à la même enseigne », a déclaré Vazquez. « Mais du même coup, cela a généré de nouvelles difficultés. Dans de nombreux domaines, le Patriot Act ne vous dit pas clairement quoi faire. Nous devons donc, comme de nombreuses banques, essayer de suivre la sophistication croissante des blanchisseurs et des terroristes, mais aussi les attentes de plus en plus grandes des organismes de réglementation. Par conséquent, nous avons augmenté nos investissements en moyens technologiques et en personnel. »

Les banques ne veulent pas violer la loi, mais plus encore, elles ne veulent pas passer pour la banque qui n'a pas détecté les activités bancaires d'un groupe terroriste. « Ce serait désastreux pour la réputation et la confiance accordée à un établissement financier – et, outre le fait qu'il faille se conformer aux réglementations, l'élément essentiel qui motive nos investissements anti-blanchiment d'argent est le suivant : protéger une réputation que Provident Bank a construit en plus de 120 ans », a déclaré Vazquez.

Les technologies avancées permettent aux établissements financiers, tels que Provident Bank, de passer au crible plus systématiquement l'identité d'un client et de surveiller les activités bancaires potentiellement suspectes. Par ailleurs, des systèmes d'analyse du comportement sophistiqués permettent de créer des profils à risque pour les clients et les employés, ce qui peut s'avérer utile dans le processus de surveillance. Pour compléter ses efforts internes, Vazquez étudie les meilleures pratiques établies par des organisations comme l'ACFE pour y trouver des informations et des formations en cours.

Vazquez utilise une gamme de logiciels d'exploration de données puissant qui permet à son organisation d'explorer des rapports publics associés à un client dont les transactions ont suscité l'attention. Ce logiciel permet aussi à la banque d'identifier des associations avec d'autres individus susceptibles de faire partie d'un réseau de blanchiment d'argent.

« Avant l'arrivée de ces technologies, une enquête interne aurait nécessité l'analyse de centaines ou de milliers de documents », a déclaré Vazquez. « Aujourd'hui, les outils d'exploration de données nous permettent d'explorer une hypothèse en quelques heures ou en quelques minutes, ce qui nous donne une image plus claire des personnes reliées à des transactions anormales.

« À cause du 11 septembre, les règles du jeu changent sans arrêt », a-t-il ajouté. « Les organismes de réglementation demandent de plus en plus de choses d'année en année. Ils veulent que vous deveniez plus efficaces, rentables, et plus sophistiqués. En fait, on y est obligés car les blanchisseurs et les terroristes repoussent eux-mêmes sans arrêt les limites. »

Toutes les organisations ont du mal à déterminer le retour sur investissement pour des investissements technologiques. Alors qu'il se préparait à assister à un conseil d'administration, Vazquez a été confronté à cette question : « Combien coûte un investissement technologique destiné à tracer des activités de blanchiment d'argent, si on se base sur les meilleures pratiques de l'industrie, par rapport à ce que ça coûte de se conformer au niveau minimum en se basant sur les réglementations du BSA et du Patriot Act ? »

Quelques heures à peine avant le début du conseil d'administration, au cours duquel Vazquez devait répondre à cette question, un article est paru, citant plusieurs banques régionales qui faisaient l'objet d'une enquête par les autorités fédérales parce qu'elles n'avaient pas détecté les activités de blanchiment d'argent d'un réseau du crime organisé relié au terrorisme.

« Notre banque ne figurait pas dans l'article car nos systèmes avaient détecté ce réseau », a déclaré Vazquez. « Pour moi, c'est le meilleur retour sur investissement : garder la réputation de notre société. »

IDENTIFIER ET ÉTUDIER LE BLANCHIMENT D'ARGENT

Tandis que les organismes d'application de la loi aux niveaux local, du comté, de l'État et fédéral mènent une lutte apparemment pénible contre le blanchiment d'argent, on peut se demander qui est vraiment mêlé à ces types d'activités criminelles. On imagine un dealer solitaire, un souteneur ou même un jeune accro à Internet qui se retrouve dans le pétrin après avoir transféré de l'argent dans un jeu en ligne.

Mais, en vérité, le blanchiment d'argent aujourd'hui est aussi organisé et discipliné que les opérations d'une grande société. Il est souvent lié à un nombre croissant d'opérations cybercriminelles sophistiquées qui évitent de se salir les mains en faisant couler le sang dans la rue.

Selon Keith Mularski, un agent spécial du FBI qui travaille dans les bureaux de la National Cyber-Forensics and Training Alliance, les groupes du crime organisé à travers le monde gèrent partout des réseaux de cybercrime qui utilisent les moyens technologiques les plus sophistiqués qui existent. En 2011, dans un article du Guardian étudiant le profil de Mularski, l'auteur Dominic Rushe écrit : « Ce sont de grands criminels qui font ça. Les activités traditionnelles du crime organisé, comme le racket ou la prostitution, ne disparaissent pas, [a déclaré] Mularski, mais les nouveaux criminels ont tout autant envie de prospérer sur Internet que leurs concurrents légitimes. »

En d'autres termes, si vous imaginez un jeune Matthew Broderick en train de pirater un site Internet gouvernemental dans le film War Games, vous vous trompez complètement.

Afin de lutter contre ce problème, les établissements financiers et les organismes d'application de la loi dans tout le pays, à tous les niveaux, reconnaissent le besoin d'investir dans des technologies qui permettraient à ces organisations de repérer plus rapidement les transactions suspectes et de réunir avec plus d'efficacité des informations sur des personnes suspectées. Comme l'a constaté le *Money Services Guide to Money Laundering Prevention* du FinCEN : « L'action fédérale visant à réduire les activités de blanchiment d'argent se concentrait autrefois essentiellement sur l'identification et la documentation de transferts de devises importants. Plus récemment, les efforts contre le blanchiment d'argent se concentrent sur l'utilisation des transferts d'argent, par l'intermédiaire de systèmes de transfert d'argent tant bancaires que non bancaires, et sur d'autres moyens de transférer des fonds. Aujourd'hui, les blanchisseurs devenant de plus en plus avertis, tous les types de transactions financières font l'objet d'une surveillance plus pointue. »

« L'obstacle le plus grand pour mener la lutte contre le blanchiment d'argent, ce sont les données », ajoute Thomas. « Il y a trop de données. Des billions de transactions ont lieu à travers les systèmes financiers du monde entier. C'est là que la technologie nous aidera à mener ce combat. »

Les recherches dans les archives nationales, dans les tribunaux de comté, ont été remplacées par des outils d'exploration de données puissants qui permettent aux organismes d'application de la loi d'analyser plus en profondeur les données pour obtenir des informations sur des activités criminelles suspectes et des personnes suspectées.

C'est un point essentiel car les blanchisseurs avertis savent comment transférer de nombreux petits montants par l'intermédiaire des systèmes financiers du monde entier pour éviter de se faire repérer. Mais un grand nombre de petites transactions finissent par faire une montagne de données qu'il faut trier.

« En tant qu'analyste financier au National White Collar Center et, précédemment, au Henrico County Police Department [Virginie], il me fallait des mois pour obtenir et compulser les archives », a déclaré Williamson. « Aujourd'hui, avec des outils tels que CLEAR, nous avons les moyens d'obtenir des tonnes de données en quelques minutes ou quelques heures. Et nous avons la possibilité de les trier pour obtenir les informations vraiment importantes. »

David Thomas (aucun lien de parenté avec Jason Thomas) recommande aux établissements financiers d'envisager l'utilisation de technologies de profilage pour mieux comprendre les blanchisseurs et les moyens de les arrêter, dans son livre blanc de 2012 « The Practice of Profiling », pour le groupe Thomson Reuters Accelus™.

« Certains organismes d'application de la loi ont analysé l'utilisation de blanchisseurs dans des affaires classées afin d'identifier des profils communs,

comme les associés criminels, les racines ethniques, familiales, géographiques, les méthodes privilégiées, etc. Les résultats sont utilisés pour remplir les bases de données des renseignements généraux, parfois pour générer de nouvelles recherches pouvant être utilisées lors de procès au titre de preuves d'association. »

Même si les petits organismes locaux et nationaux ont les technologies dont ils ont besoin pour identifier et enquêter sur le blanchiment d'argent et les cybercrimes qui y sont associés, ils n'ont pas toujours la formation exigée pour profiter pleinement de ces technologies, a remarqué Williamson. Ce manque de formation est dû à plusieurs raisons.

« L'un des problèmes est le coût des formations spécialisées », a déclaré Williamson. « La formation en technologie coûte souvent entre 3 000 $ et 5 000 $ pour une semaine et il faut des fonds supplémentaires pour acheter le logiciel et les outils nécessaires pour mener à bien les enquêtes en cours. »

Afin d'aider les organismes d'application de la loi qui luttent pour trouver les fonds nécessaires à la formation anti-blanchiment d'argent, le NW3C propose des formations gratuites aux organismes membres dans tout le pays. L'an dernier, le NW3C a proposé des formations à plus de 6 500 membres du personnel assermentés (et plus de 50 000 membres du personnel assermentés depuis 1996). Par ailleurs, le NW3C aide les organismes d'application de la loi en proposant des outils d'investigation gratuits tels que Microsoft® COFEE (Computer Online Forensic Evidence Extractor), PerpHound™ (un outil de science légale qui permet aux enquêteurs d'analyser les données d'appels des opérateurs téléphoniques) et NW3C TUX4N6™ (un CD de démarrage qui permet aux organismes d'application de la loi de prévisualiser un disque dur sans enregistrer ni modifier de données sur le système).

DIFFICULTÉS ET OPPORTUNITÉS

Dans l'univers du blanchiment d'argent, la lutte entre les criminels et les établissements financiers et les organismes d'application de la loi ressemble à une partie d'échec. Une attaque est suivie d'une contre-attaque. L'un des joueurs essaie d'éviter l'autre. Au fur et à mesure que les pièges surgissent, l'adversaire en tire la leçon et met en place de nouvelles compétences et de nouvelles stratégies.

À cause des réglementations et de leur désir d'éviter de perdre la confiance de leurs clients, les banques font de lourds investissements dans les technologies pour surveiller les transactions et apprendre à connaître leurs clients. De même, les organismes d'application de la loi fédéraux et, dans une certaine mesure, les organismes d'application de la loi de l'État et locaux, complètent ces investissements par des technologies de police prédictive et d'enquêtes juridiques qui leur permettent de voir, au-delà des individus, des réseaux et des sociétés entiers susceptibles d'être mêlés au blanchiment d'argent et à d'autres activités criminelles.

Si les établissements financiers continuent à augmenter les contrôles sur leurs systèmes de transactions, les organisations criminelles, en réaction à ces contrôles plus stricts, chercheront d'autres systèmes pour blanchir leur argent. Cependant, un grand nombre de ces systèmes ne semblent pas être aussi efficaces pour traiter des sommes d'argent importantes que les banques traditionnelles ou en ligne.

Et ceux qui sont presque aussi efficaces que les banques, comme les casinos, évoluent en matière de contrôles anti-blanchiment d'argent. À la fin du mois de janvier 2013, la Las Vegas Sands Corp. a annoncé qu'elle avait cessé ses transferts d'argent internationaux et qu'elle remaniait ses procédures de conformité, selon le Wall Street Journal (Kate O'Keefe, 24 janvier 2013), dans le cadre de ses négociations avec les autorités fédérales pour dissiper des allégations de blanchiment d'argent. La FATF a demandé des contrôles anti-blanchiment d'argent supplémentaires pour les casinos, surtout dans les points chauds connus pour le blanchiment d'argent tels que les Philippines et Macao (qui est devenu un port offshore pour les blanchisseurs chinois).

Transformer de l'argent avec les jeux en ligne ou des devises numériques peut offrir des alternatives qui ne vont pas sans risques. Dans l'affaire E-Gold Ltd de 2007, un fournisseur de devises numériques qui proposait un système de paiement basé sur l'anonymat et financé par des réserves d'or et d'argent, le gouvernement américain a manifesté sa volonté d'attaquer une société émettrice de devises numériques qu'il soupçonnait servir de système international de blanchiment d'argent, ce qui fut prouvé lors du procès. L'affaire E-Gold prouva que les criminels cherchent sans arrêt des sources pour stocker et déplacer de l'argent, mais qu'au final, ils veulent tout de même utiliser des devises fiables, répandues et souveraines comme les dollars américains ou les euros.

Si les devises sont le point essentiel dans la lutte incessante entre les criminels et les organismes d'application de la loi, il semblerait que les criminels se ruent en masse vers les devises numériques plus sûres qui vont être introduites dans les années à venir. La Suède, premier pays à avoir introduit les billets en papier en 1661, se dirige vers une société sans argent liquide. Et l'an dernier (en août 2012), la Royal Bank of Canada a introduit la MintChip, l'équivalent numérique de sa devise version papier.

Il va sans dire que si les gouvernements souverains se mettent à écouler des devises numériques, la compétition risque d'écraser les devises privées comme Bitcoin ou des devises futures. Néanmoins, si les devises souveraines pouvaient être tracées à des fins d'anti-blanchiment d'argent ou même fiscales, l'expérience passée montre que le marché des cryptodevises privées continuera à exister et à proliférer.

La mutation au sein des cryptodevises privées exige le maintien de l'anonymat entre les individus et les organisations. Par exemple, si les dealers sont prêts à accepter un paiement en devises numériques pour un sachet d'héroïne via un téléphone mobile ou un site Internet, les deux parties, à savoir le dealer et l'acheteur, veulent garantir leur anonymat en ligne, même si les devises numériques peuvent être tracées via un codage crypté.

Partant de ce point de vue, le plus gros obstacle auquel les organismes de réglementation et d'application de la loi risquent d'être confrontés est le nombre croissant de lois sur la confidentialité créées pour répondre aux exigences d'un monde numérique. Si un dealer décide de circuler dans des environnements contrôlés, comme les banques, qui ont l'obligation de « connaître leur client », selon David W. Blass, conseiller en chef à la Division of Trading and Markets de la Securities and Exchange Commission (SEC), dans son article du Securities Technology Monitor de mars 2012, « Past and Future of Fighting Money Laundering » (Passé et avenir de la lutte contre le blanchiment d'argent), à quel moment les gouvernements d'État ou fédéraux peuvent-ils intervenir pour dévoiler l'identité des individus en ligne ?

Tandis que les établissements financiers, les agences gouvernementales et les organismes d'application de la loi se demandent comment lutter contre le blanchiment d'argent de manière efficace et organisée, d'autres problèmes connexes peuvent se présenter dans les années à venir du fait que les groupes du crime organisé deviennent de plus en plus habiles pour déplacer de l'argent dans un monde numérique. Parmi ces problèmes, on peut citer :

L'éducation – Williamson, du NW3C, pense qu'un grand nombre d'organismes d'application de la loi ne sont pas préparés pour gérer la nouvelle réalité du cybercrime et les méthodes sophistiquées que les groupes du crime organisé utilisent pour blanchir de l'argent. Une formation et une éducation approfondies à tous les niveaux sont nécessaires, notamment dans les commissariats de police dans les petites villes et les communautés rurales du comté. Une formation peut contribuer à surmonter sa peur d'être confronté à de nouvelles technologies et à l'énorme quantité de données typiques des affaires de blanchiment d'argent.

L'avertissement – De même, les banques et les autres établissements financiers doivent continuer à investir dans des formations « Avertissement » pour les employés de première ligne qui manipulent des fonds ou qui ouvrent des comptes, afin qu'ils reconnaissent les signes d'un blanchiment d'argent au quotidien. Comme le notait Jennifer Shasky Calvery, directrice du FinCEN, dans ses remarques du 27 février 2013 à la Securities Industry and Financial Markets Association (SIFMA), « le FinCEN élabore la défense, mais c'est aux établissements financiers de la construire et de la mettre à exécution au quotidien. »

Les autres devises – Selon le FBI, si la popularité des devises numériques continue à augmenter, elles attireront de plus en plus d'éléments du monde criminel qui veulent éviter les systèmes financiers traditionnels pour faire des transferts d'argent. Tant que certaines devises numériques pourront continuer à maintenir l'anonymat, tout en devenant plus courantes (faciles à acquérir par des transferts simples d'argent réel), les organismes d'application de la loi auront de plus en plus de mal à tracer ces transactions.

Le rôle imprévisible des hacktivistes – Les activités d'Anonymous et d'autres mouvements hacktivistes au sein du Web invisible sont un facteur imprévisible dans le contrôle et l'examen du blanchiment d'argent, si on se réfère à d'autres incidents et problèmes auxquels Anonymous a été mêlé. À un moment donné, ces groupes contribueront-ils à aider les organismes d'application de la loi à identifier les groupes criminels ou, en se référant à leurs systèmes de croyances, mettront-ils des bâtons dans les roues

des organismes d'application de la loi au nom de la liberté de la vie privée ?

Le partage des informations – Pour lutter contre la menace actuelle du blanchiment d'argent et du financement du terrorisme, il faut absolument que les organismes d'application de la loi et les établissements financiers, aux niveaux fédéral, de l'État et local, s'associent pour travailler en étroite relation ensemble. Un partage des informations rapide et efficace est la solution pour arrêter le développement du blanchiment d'argent. Les agences gouvernementales devront continuer à investir dans les technologies de l'information pour augmenter les possibilités d'accès aux données. FinCEN Query, qui a été lancé en septembre 2012, est une étape dans la bonne direction, selon Calvery. Cette technologie donne aux organismes d'application de la loi l'accès aux données du BSA sur les 11 dernières années. Et pour finir, les organismes d'application de la loi doivent investir dans des technologies d'investigation qui leur permettent d'analyser plus en profondeur ces données pour optimiser leurs systèmes d'investigation.

Les droits à la protection de la vie privée – Les organismes d'application de la loi et les élus doivent s'attendre à des réactions virulentes de la part des défenseurs des droits à la protection de la vie privée qui se demandent avec appréhension jusqu'où peut aller la surveillance en ligne des organismes d'application de la loi et quel genre de données ils sont en droit d'exiger de la part des fournisseurs Internet quand ils recherchent des organisations criminelles et des blanchisseurs.

Un budget adapté aux technologies et aux personnes – Pour lutter efficacement contre le blanchiment d'argent, il faut absolument que les organismes d'application de la loi et les agents du risque des entreprises aient les moyens de surveiller et d'étudier toute activité suspecte. Cependant, de nombreux organismes d'application de la loi étant soumis à de plus en plus de pressions pour conserver ou réduire les budgets existants, les organismes risquent d'être obligés de transiger sur les investissements dans les technologies et le personnel spécifiquement formé aux technologies d'investigation sur les actions de blanchiment d'argent.

Éviter le déni – Blass, de la SEC, a noté dans un article récent du Security Technology Monitor, que la mise en place par les établissements financiers de programmes anti-blanchiment d'argent n'est pas suffisante. Les personnes doivent être formées à se manifester quand elles soupçonnent un comportement suspect, même si cela entraîne la perte possible d'un compte rentable.

ÉVÉNEMENTS MARQUANTS DE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT

1970 – Le Bank Secrecy Act (BSA) devient une loi qui débouche sur la création d'un système d'information comptable pour les transactions supérieures à 10 000 $, constituant une étape dans le contrôle du flux des recettes obtenues de façon illégale. Source : Westlaw.

1970 – Le Racketeer Influenced and Corrupt Organizations (RICO) Act définit le blanchiment d'argent comme étant une infraction sous-jacente représentant une activité de racket. Source : Westlaw.

1986 – Le Money Laundering Control Act amende le BSA et définit le blanchiment d'argent comme étant un crime fédéral. Source : Westlaw.

1988 – L'Anti-Drug Abuse Act fixe des peines et des sanctions pour les activités de blanchiment d'argent, en amendant les clauses relatives aux tentatives d'évasion fiscales et à l'enregistrement de fausses déclarations fiscales. Source : Westlaw.

1989 – Le Fonds Monétaire International (FMI) forme la Financial Action Task Force on Money Laundering (FATF), une agence gouvernementale internationale composée de 36 membres, créée par le sommet du G7 à Paris pour mettre en place une norme internationale en matière de lutte contre le blanchiment d'argent et contre le financement du terrorisme (CFT).

1992 – L'Annunzio-Wylie Anti-Money Laundering Act renforce le BSA, ce qui exige la vérification et l'archivage des virements bancaires. Source : Westlaw.

1994 – Le Money Laundering Suppression Act demande aux banques de mettre en place des procédures d'examen anti-blanchiment d'argent et demande l'enregistrement des sociétés de services de paiement (MSB ou Money Services Business). Cette loi considère comme un crime fédéral le fait de diriger une MSB non enregistrée.

1998 – Le Money Laundering and Financial Crimes Strategy Act exige du ministre des Finances qu'il mette en œuvre un plan national pour régler le problème du blanchiment d'argent. Source : Westlaw.

2001 – Le USA Patriot Act crée de nouvelles réglementations pour empêcher, détecter et punir le

terrorisme et le blanchiment d'argent international dans les sociétés et les établissements financiers. Cette loi exige des banques qu'elles surveillent les transactions et elle augmente les sanctions administratives et les peines criminelles en cas de blanchiment d'argent. Source : Westlaw.

2002 – Le ministère des Finances américain publie le rapport National Money Laundering Strategy destiné à définir le rôle du blanchiment d'argent dans la guerre contre le terrorisme.

2004 – Le Bank Secrecy Act (BSA) a été amendé avec l'adoption de l'Intelligence Reform and Terrorism Prevention Act de 2004, qui crée des réglementations exigeant de certains établissements financiers qu'ils signalent les transferts de fonds électroniques internationaux. Source : Westlaw.

2005 – La Drug Enforcement Agency (DEA) termine Operation Mallorca, une enquête marquante, relative au blanchiment d'argent, sur le Colombian Black Market Peso Exchange. Cette opération s'est terminée par l'arrestation de 36 personnes, la saisie de 7,2 millions de dollars, plus de 10 000 kg de marijuana, 947 kg de cocaïne et 7 kg d'héroïne. Source : NW3C.

Références

Interview, Cindy Williamson, CFE, CAMS, enforcement analyst III, National White Collar Crime Center (NW3C), avril 2013.

"Fitch: More Banks Facing U.S. Anti-Money Laundering Scrutiny", Fitch (communiqué de presse), 5 avril 2013.

"The IMF and the Fight Against Money Laundering and the Financing of Terrorism", Fonds Monétaire International, 31 mars 2013.

Interview, Jason Vazquez, senior vice president et BSA/ AML compliance officer, Provident Bank, mars 2013.

Interview, Jason Thomas, senior strategic analyst, Thomson Reuters, mars 2013.

Interview, Katherine Sagona-Stophel, government analyst, Thomson Reuters, mars 2013.

"Web Money Gets Laundering Rule", Jeffrey Sparshott, Wall Street Journal, 21 mars 2013.

"Eye on Digital Currency: Amazon Sellers Get Bitcoin Option; Hackers Steal Bitcoins", Digital Transactions, 11 mars 2013.

"History of Anti-Money Laundering Laws", Financial Crimes Enforcement Network, ministère des Finances américain, 2013.

"Bitcoin Looks Primed for Money Laundering", Cyrus Sanati, Fortune.com/CNNMoney.com, 18 décembre 2012.

"HSBC to pay $1.9 billion U.S. fine in money-laundering case", Aruna Wiswanatha et Brett Wolf, Reuters.com, 11 décembre, 2012.

"Welcome to the Deep Web: The Internet's Dark and Scary Underbelly", Pablo Albarracin et Christopher Holloway, Worldcrunch.com, 17 novembre 2012.

"U.S. Treasury to Lead Review of Anti-Money Laundering Rules", Brett Wolf, Reuters, 12 novembre 2012.

"Minting the Digital Currency of the Future", David Wolman, Wired.com, 7 mai 2012.

"Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity", Intelligence Assessment, Federal Bureau of Investigation, 24 avril 2012.

"Money Laundering and Asset Forfeiture: Taking the Profit Out of Crime", Douglas Leff, J.D., FBI Law Enforcement Bulletin, avril 2012.

"New Payment Methods and Financial Crimes Risk", David Thomas, Thomson Reuters Accelus, janvier 2012.

"General Questions: What Is Money Laundering?" Financial Action Task Force (FATF), 2012.

"The Practice of Profiling, Part 3", David Thomas, Thomson Reuters Accelus, 2012.

"Examples of Money Laundering Investigations, Fiscal Year 2011", Internal Revenue Service (IRS), 2011.

"Alternative Currencies Grow in Popularity", Judith D. Schwartz, TIME Magazine, 14 décembre 2008.

"Money Laundering", National White Collar Crime Center, mai 2006.

THOMSON REUTERS ACCELUS™

La division Gouvernance, Risque et Conformité (GRC) de Thomson Reuters propose un ensemble très complet de solutions conçues pour donner aux professionnels de l'audit, du risque et de la conformité, aux dirigeants d'entreprise, ainsi qu'à leurs conseils d'administration, les moyens de réaliser leurs objectifs métier, de gérer l'incertitude et d'agir avec intégrité.

Thomson Reuters Accelus permet d'accorder les transactions commerciales, la stratégie et les opérations à un environnement réglementaire en mutation permanente, de façon à permettre aux entreprises de gérer au mieux leurs risques métier. Accelus est une plateforme complète servie par un large éventail d'applications, ainsi que par des données d'une grande fiabilité en matière de veille réglementaire et de risque. Elle regroupe les meilleures solutions du marché dans les domaines suivants : gouvernance, gestion des risques et de la conformité, veille réglementaire mondiale, criminalité financière, lutte contre la corruption, renforcement des efforts de due diligence, formation et e-learning, et services aux conseils d'administration et d'information.

Thomson Reuters a été nommé leader de sa catégorie dans le classement Chartis RiskTech Quadrant™ pour les systèmes de gestion des risques opérationnels ; et leader de sa catégorie dans le classement Chartis RiskTech Quadrant™ pour les systèmes de gouvernance d'entreprise, de gestion du risque et de conformité. Thomson Reuters a également été placé dans le quadrant leader du Magic Quadrant de Gartner, Inc. pour les plateformes de gouvernance d'entreprise, de gestion du risque et de conformité. Thomson Reuters s'est par ailleurs vu décerner le prix du fournisseur de logiciels de gestion du risque opérationnel de l'année, dans le cadre des Operational Risk and Regulation Awards 2013.

For more information, visit accelus.thomsonreuters.com

THOMSON REUTERS™

© 2013 Thomson Reuters GRC00403_FR/12-13