Prévention des fraudes au sein des organismes sans but lucratif

La fraude est un problème important qui peut avoir des répercussions sur n'importe qui, des individus aux grandes entreprises en passant par les associations.

Pour un groupe sans but lucratif comme le vôtre, la fraude — tant à l'interne qu'à l'externe — peut être particulièrement catastrophique. Elle peut non seulement avoir une incidence sur la capacité de votre organisation à remplir son mandat financier, mais également ternir son image auprès du public. Cette situation pourrait entacher votre réputation, saper votre crédibilité, créer un déficit de financement à plus long terme et mener à d'autres problèmes.

Il existe un certain nombre de mesures à prendre pour minimiser la possibilité de fraude et ses répercussions négatives sur votre organisme. Comprendre les différents types d'activités frauduleuses et offrir de la formation à cet égard à votre personnel ainsi qu'à vos associés en indiquant notamment comment la fraude peut se produire et quelles sont les meilleures façons de la contrer est un bon début. Vous pourrez ensuite intégrer des procédures à l'aide de vérifications et de garde-fous pour empêcher toute activité frauduleuse.

L'importance des contrôles internes

Les juricomptables disent que lorsqu'une fraude se produit, elle n'est généralement pas repérée à l'interne — elle est plutôt découverte en raison de renseignements obtenus ou tout simplement par accident.

On estime qu'entre janvier 2014 et décembre 2016, les Canadiens ont perdu plus de 290 millions de dollars aux mains de fraudeurs[1].

Une récente étude effectuée par l'Association of Certified Fraud Examiners a établi une corrélation entre la présence de mesures antifraudes d'une part et la diminution des pertes sur fraudes et la détection rapide des fraudes d'autre part. En comparant les organismes qui disposent de mesures antifraudes à ceux n'en disposent pas, nous avons constaté que, lorsque des mesures sont en place, les pertes sur fraudes sont de 12 % à 56 % inférieures et que les fraudes sont détectées plus rapidement[2]. Lorsqu'un employé ou un bénévole constate des lacunes qu'il peut exploiter à son avantage, il peut être difficile d'y résister. Il faut aussi savoir que la fraude peut toucher jusqu'à 5 % des revenus d'un organisme[3]. Il est donc essentiel que les organismes connaissent les signaux d'alarme, établissent des procédures et prennent des précautions très précises pour éviter la fraude — des procédures et précautions visant tout particulièrement les personnes qui manipulent le numéraire.

Mesures de prévention de la fraude — Comment établir des contrôles internes

Séparer vos tâches liées au traitement des paiements

- Il faut, si possible, éviter qu'une seule personne soit responsable du numéraire, de l'émission des chèques ou de la conciliation des relevés bancaires.
- Avoir deux signataires pour l'émission des chèques s'avère une bonne pratique.
- Si des modifications sont apportées à l'égard des signataires, s'assurer de les documenter et de les indiquer sur les formules d'autorisation bancaire.

Mettre en place des procédures rigoureuses de manipulation du numéraire

- Effectuer rapidement les dépôts en utilisant les services de dépôt de nuit, 24 heures sur 24 et sept jours sur sept.
- Émettre des paiements individuels pour les dépenses afin que chaque paiement puisse être lié à une facture précise.
- Garder les chéquiers, le numéraire et les relevés bancaires, ainsi que les chèques annulés, dans un endroit verrouillé.
- Penser à utiliser des cartes de crédit ou des paiements électroniques plutôt que des chèques pour effectuer les paiements.
- Rapprocher tous les paiements avec la facture du fournisseur ou tout autre document papier.

Vérifier les antécédents des employés

- Effectuer une vérification de base des antécédents de tous les associés – qu'ils soient à salaire ou non.
  - Contacter les références indiquées, tant personnelles que professionnelles.
  - Penser à effectuer des vérifications pour déceler toute activité criminelle.
- Exiger le versement d'une caution par les personnes qui manipulent du numéraire.

Implanter des méthodes comptables

- Si vous avez des vérificateurs, leur demander de mettre en place une politique d'audit pour faciliter la détection de toute comptabilité ou tenue de livres frauduleuse.

Prévenir la fraude par chèque

- Refuser d'accepter tout chèque dont vous ne pouvez prouver la légitimité.
- Vérifier la date ainsi que la signature et rechercher toute modification apportée à un chèque, comme un changement du montant en dollars.
- Garder un contrôle serré sur vos propres chèques.
- Effectuer fréquemment le rapprochement des relevés bancaires — la meilleure pratique consiste à le faire chaque jour.

Protéger votre marque contre le vol d'identité

- Toujours tenter de déceler les « pirates » qui peuvent s'attaquer à votre identité ou à votre marque et utiliser l'identité de votre association ou celle d'autres organismes de bienfaisance reconnus pour solliciter et obtenir des fonds.
- Encourager les associés, les donateurs et le public à déclarer toute communication ou demande suspecte.

Protéger votre infrastructure informatique

Vos systèmes informatiques contiennent tous les éléments essentiels à votre organisme : l'information sur les donateurs/membres, les données financières et plus encore. Il est donc vital que vous mettiez en œuvre une politique de sécurité informatique qui régit l'utilisation de toutes les données, de tous les serveurs et de tous les réseaux et qui couvre le matériel, comme les ordinateurs portables et les lecteurs externes. Cela est particulièrement important dans les cas où les associés travaillent à l'extérieur ou en dehors des heures normales de bureau. Une surveillance régulière du système, y compris des courriels, constitue à la fois une défense et une mesure de dissuasion.

Pour éviter les brèches de sécurité dans les TI :

- Sécuriser tous les ordinateurs – tout particulièrement les ordinateurs portables.
- Établir un protocole de sécurité de l'information pour les graveurs de CD/DVD et lecteurs externes.
- Ne jamais répondre aux courriels demandant l'envoi d'un mot de passe (aussi appelés « hameçonnage » ou « mystification »).

Si vous soupçonnez une fraude, veuillez immédiatement :

- Débrancher la source utilisée pour l'intrusion
- Isoler les systèmes corrompus

- Arrêter les serveurs ou concentrateurs visés pour éviter tout autre accès au système
- Communiquer avec votre fournisseur de service Internet ou votre fournisseur d'accès pour tenter de retracer l'attaque
- Dans le cas de brèches importantes de sécurité, penser à communiquer avec la police

Conseils pour éviter la fraude par courrier

Courrier entrant

- Si vous soupçonnez un vol de courrier, aviser votre bureau de poste local et la police.
- Récupérer rapidement tout le courrier reçu.
- S'assurer que votre boîte aux lettres est verrouillée (le cas échéant).
- Remplacer vos boîtes aux lettres installées sur le mur par un passe-lettres.
- Nommer une personne responsable de toutes les tâches connexes au courrier.
- S'assurer que l'endroit où est déposé le courrier est toujours bien en vue.

Courrier sortant

- Ne jamais laisser de courrier sortant dans votre boîte aux lettres.
- Éviter les boîtes aux lettres sur la rue.
- Envoyer les chèques d'un montant élevé par courrier recommandé ou utiliser le télévirement.

Signes qu'un chèque est douteux

- Le nom de la banque émettrice, son adresse, etc. ne figurent pas sur le chèque.
- Le mot « Annulé » est indiqué sur le chèque.
- Le chèque n'est pas signé.
- Les numéros MICR indiqués au bas du chèque sont manquants ou ne correspondent pas au numéro de série du chèque.
- Des taches ou une décoloration peuvent indiquer des tentatives d'altération.
- Le numéro de chèque est manquant ou n'a pas changé.
- Problèmes à l'égard des caractères utilisés (l'écriture du nom ne correspond pas à celle de l'adresse ou du montant, etc.).

À propos de l'escroquerie par intrusion dans un courriel d'entreprise

L'escroquerie par intrusion dans un courriel d'entreprise commence souvent lorsqu'un fraudeur réussit à compromettre un employé de haut niveau ou un dirigeant de l'entreprise en ce qui concerne les finances ou un compte de courriel public. Ce type de fraude est normalement fait à l'aide de méthodes d'hameçonnage ou de logiciels malveillants qui enregistrent les mots de passe. Le fraudeur crée alors un domaine semblable à celui de l'entreprise ciblée (ou un courriel mystifié) pour amener sa cible à fournir des renseignements sur le compte.

En surveillant le compte de courriel visé par la fraude, le fraudeur essaiera de déterminer qui fait des télévirements et qui les demande. Les auteurs de ce type de fraude effectuent souvent beaucoup de recherches, cherchant les entreprises qui ont connu un changement au sein de la direction, qui ont annoncé publiquement une fusion/acquisition ou qui ont entrepris un projet de rénovation ou un projet immobilier important. Ils profitent alors de l'événement pour commettre une fraude.

Quelques escroqueries courantes par intrusion dans un courriel d'entreprise

- **Fausse facture** – Les fraudeurs utilisent souvent cette tactique pour cibler les entreprises ayant des fournisseurs à l'étranger. L'attaquant se fait passer pour un fournisseur et demande que des paiements soient effectués par virements de fonds à un compte détenu par le fraudeur.
- **Escroquerie au chef de la direction** – L'attaquant se fait passer pour le chef de la direction ou un cadre supérieur de l'entreprise et envoie un courriel aux employés du service des finances pour leur demander de virer des fonds au compte du fraudeur.
- **Compromission de compte** – Le compte de courriel d'un employé ou d'un dirigeant est piraté et utilisé pour demander que des paiements soient effectués aux fournisseurs figurant dans la liste de contacts. Les paiements sont alors envoyés à des comptes bancaires frauduleux.

- **Usurpation de l'identité d'un avocat** – L'attaquant se fait passer pour un avocat ou un employé d'un cabinet d'avocats soi-disant chargé de questions importantes et confidentielles. De telles demandes fictives sont habituellement faites par courriel ou par téléphone, à la fin d'un jour ouvrable.
- **Vol de données** – Les fraudeurs ciblent les employés des RH ou de la tenue de livres afin d'obtenir des renseignements personnels identifiables ou des relevés fiscaux d'employés et de dirigeants. Ces données peuvent être utilisées pour des attaques ultérieures.

Puisque ces fraudes ne comprennent aucune pièce jointe ni aucun lien malveillant, elles peuvent échapper aux solutions traditionnelles. La formation et la sensibilisation des employés peuvent aider les entreprises à repérer ce genre de fraude.

Repérage de l'hameçonnage et de la mystification de marque

Il s'agit d'une technique qui consiste à envoyer un courriel semblant provenir d'une société légitime afin d'obtenir des renseignements personnels ou financiers. L'adresse de courriel est modifiée afin de ressembler de très près à une adresse de courriel légitime.

Exemples :

- Légitime : Companyname.com
  Modifiée pour : Companyname.us (« .com » est remplacé par « .us »)
- Légitime : Companyname.com
  Modifiée pour : Companynarne.com (le « m » est remplacé par le « r » et le « n »)

Établir les protocoles d'authentification

La présente procédure vise à vérifier la demande d'un expéditeur concernant le paiement ou la modification des instructions permanentes.

Un simple appel téléphonique au numéro indiqué au dossier peut nous permettre de confirmer si les modifications demandées sont légitimes et si des paiements importants ont été autorisés. Cela vous sera très utile pour éviter les décaissements non autorisés et les opérations frauduleuses ou douteuses.

Vous pouvez utiliser les protocoles d'authentification lorsque :

- Une télécopie, une lettre ou un appel téléphonique semble anormal ou non conforme aux opérations antérieures
- Des instructions ont été envoyées par courriel ou par message texte (même si le numéro de téléphone ou l'adresse de l'expéditeur semble valide)
- Un sentiment d'urgence est manifesté
- Le montant demandé dépasse la limite interne établie

Nous sommes très fiers de la tradition de RBC Banque Royale de participation à la collectivité, de financement d'événements spéciaux et de lien avec de nombreuses initiatives philanthropiques. Nous comprenons donc bien les besoins particuliers des associations d'organismes sans but lucratif. Notre équipe de directeurs nationaux chargés des organismes sans but lucratif peut vous offrir des solutions rentables, y compris des outils de gestion de l'encaisse et des placements, conçues pour maximiser vos ressources.

Saines pratiques commerciales

- Mettre officiellement en place un code de déontologie.
- Rédiger une politique appropriée sur les dépenses.
- Fermer le ou les comptes en cas de vol présumé de relevés de carte de crédit ou de relevés bancaires.
- Ne pas utiliser les numéros d'assurance sociale (NAS) comme numéro d'employé.
- Offrir au personnel de la formation sur la prévention des fraudes.
- Déchiqueter les documents contenant des données sensibles.
- Sécuriser toutes les données sensibles (identificateur d'utilisateur, numéros de compte, etc.).
- Installer un accès protégé par mot de passe aux ordinateurs et changer souvent les mots de passe.
- Changer régulièrement votre numéro d'identification personnel (NIP).
- Attribuer un mot de passe unique à chaque employé.
- Restreindre l'accès aux données en fonction de sa pertinence par rapport au poste de l'employé.
- Effectuer des vérifications au hasard dans les comptes de l'entreprise.
- Ne jamais accepter de chèques payables à un tiers.

Les conseils et les trucs présentés ici sont loin d'être complets. Il existe une foule de renseignements qui peuvent aider votre entreprise à mettre en place un protocole pour la détection et la prévention des fraudes.

Pour obtenir plus de détails sur la détection et la prévention des fraudes, ainsi que sur une vaste gamme de solutions financières pour votre organisme du secteur public, veuillez consulter le site www.rbcroyalbank.com/fr/entreprises/conseils/expertise-sectorielle.html.

[1] https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04201.html
Bureau de la concurrence Canada, gouvernement du Canada
« Fait sur la fraude 2017– Détecter, contrer et signaler la fraude »

[2] https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf
Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse, Association of Certified Fraud Examiners

[3] https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf
Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse, Association of Certified Fraud Examiners

VPS104948

57460 (07/2019)