Chambre des notaires

**DOSSIER**
FRAUDE ET BLANCHIMENT D'ARGENT
Article 2/8

# 4 types d'arnaques et mesures à prendre pour vous protéger

Les entreprises deviennent de plus en plus des proies faciles pour les fraudeurs à mesure que leurs stratagèmes se complexifient et se raffinent. Cet article explore brièvement quatre types d'arnaques visant les notaires et donne des trucs et astuces pour les reconnaître et les contrer.

## Blanchiment d'argent

Le blanchiment d'argent est le transfert, l'utilisation ou la livraison de biens ou de produits provenant d'activités criminelles dans l'intention de les cacher ou de les convertir. Les juristes présentent un intérêt grandissant pour les criminels cherchant à recycler ou à faciliter le blanchiment des produits de leur criminalité. Les domaines du droit de l'immobilier, des fiducies et du droit commercial sont particulièrement ciblés, rendant les notaires qui y exercent plus vulnérables.

Le processus de blanchiment d'argent suit trois étapes, auxquelles les blanchisseurs peuvent tenter de faire participer les notaires :

**1. LE PLACEMENT.** Le blanchisseur introduit les profits illégaux dans le système financier, par exemple en déposant l'argent dans une institution financière, en convertissant les devises dans un bureau de change ou en déposant des fonds dans le compte en fidéicommis d'un notaire.

**2. LA STRATIFICATION.** Le blanchisseur effectue une série d'opérations pour éloigner les fonds de leur source.

**3. L'INTÉGRATION.** Le blanchisseur intègre les fonds dans l'économie légitime en les investissant, notamment dans l'immobilier ou des entreprises commerciales.

### COMMENT DÉJOUER CE TYPE DE FRAUDE

- Prudence est le mot d'ordre. Le notaire ne devrait pas hésiter à poser des questions dès le premier contact, et ce, avant même d'accepter le mandat. En cas de doute, refusez le mandat et évitez de participer à des transactions frauduleuses.
- Soyez à l'affût de ces signaux : la compagnie ou le particulier n'a pas d'adresse courriel ou d'adresse postale, de numéro de téléphone à la maison ou d'affaires ; le client semble peu se soucier du bien, du prix, du taux d'intérêt hypothécaire et des frais juridiques ou de courtage et offre de payer des frais juridiques plus élevés que la normale ; une partie à l'opération est un acheteur étranger, soit un particulier ou une compagnie dont le seul lien avec le Canada est l'opération immobilière.

# Vol de titre

Cette fraude se produit lorsque le titre de propriété est dérobé, puis que le fraudeur vend la maison ou demande une nouvelle hypothèque sur celle-ci. Les cibles privilégiées par les fraudeurs sont généralement des maisons libres de dettes ou avec une grande équité, les « snowbirds » qui passent plusieurs mois dans le Sud, ou encore les enfants portant les mêmes nom et prénom que l'un de leurs parents.

Pour parvenir à leurs fins, les fraudeurs se procurent divers documents pour aliéner ou refinancer la maison (p. ex. titre de propriété, certificat de localisation, compte de taxes foncières, fausses pièces d'identité, etc.).

### COMMENT DÉJOUER CE TYPE DE FRAUDE

- Examinez minutieusement les pièces d'identité originales (p. ex. comparez la signature du client et sa taille, vérifiez son numéro d'assurance sociale sur le site du gouvernement et la validité de son permis de conduire sur celui de la SAAQ, etc.).
- Soyez à l'affût de ces signaux : l'immeuble transigé est libre de dettes; la transaction revêt un caractère urgent; la partie contractante dit s'être fait voler ses pièces d'identité et demande de procéder à la signature sur promesse de les produire rapidement; la partie fournit une copie des pièces d'identité plutôt que les originaux; un nouveau client procède à plus d'un emprunt hypothécaire; il y a incohérence (date de naissance, taille, etc.) entre les pièces d'identité.

# Extorsion par rançongiciel

Il s'agit d'une technique d'extorsion répandue auprès des entreprises. Des logiciels malveillants sont conçus pour accéder à votre ordinateur, trouver des renseignements personnels et bloquer l'accès à votre ordinateur ou à votre réseau, perturbant les activités de votre entreprise. Une demande de rançon est par la suite envoyée pour « débloquer » le tout.

Les logiciels malveillants peuvent être introduits de plusieurs façons, entre autres par l'entremise d'un lien ou d'une pièce jointe reçus dans un courriel, le téléchargement d'une application, une visite sur des sites Web moins sûrs, des publicités en fenêtres contextuelles.

### COMMENT DÉJOUER CE TYPE DE FRAUDE

- Protégez vos données à l'aide de logiciels de sécurité fiables et à jour.
- Adoptez des pratiques électroniques sécuritaires (modifiez régulièrement les mots de passe de l'entreprise, sauvegardez vos données à l'extérieur de votre réseau, etc.).
- Vérifiez attentivement l'adresse courriel de l'expéditeur puisque souvent un seul caractère diffère de la véritable adresse de votre client.
- Ne cliquez pas sur un lien ou une pièce jointe envoyé par un expéditeur que vous ne connaissez pas.

# Hameçonnage

L'hameçonnage est un type de fraude qui vous dirige vers des plateformes de communications qui semblent légitimes (p. ex. site Web d'une institution financière, courriel portant le logo d'une agence gouvernementale, etc.). En réalité, ces plateformes ont été conçues pour voler des informations personnelles telles que les numéros de carte de crédit, les numéros de comptes bancaires ou les mots de passe de l'entreprise.

Le fraudeur communique avec vous via courriel, téléphone, texto ou encore via les réseaux sociaux. Il peut se faire passer pour un représentant d'une institution financière, un client ou un organisme gouvernemental.

### COMMENT DÉJOUER CE TYPE DE FRAUDE

- Lorsque vous recevez ce type de communication, soyez très vigilant, surtout si on vous demande de cliquer sur des pièces jointes ou des hyperliens. Signalez les courriels suspects ou non sollicités comme « pourriels », puis supprimez-les.