N°2024-04 le 21 février 2024

RECRUDESCENCE DES CAS DE FAUX ORDRES DE VIREMENTS (FOVI) A L'ENCONTRE DES ETUDES NOTARIALES

Il a été constaté en 2023 une recrudescence du nombre de cas de faux ordres de virements touchant la profession des notaires. En raison des montants élevés des transactions effectuées par les études, en particulier en matière immobilière, les cabinets de notaire représentent une cible de choix pour les escrocs.

On distingue **3 modes opératoires principaux :**

1. L'arnaque dite au « faux président » :

Initialement conçue pour piéger les grandes entreprises, cette arnaque a été adaptée aux études notariales. L'escroc appelle le service comptable de l'étude et se présente comme un avocat ou un consultant travaillant sur un projet sensible pour l'associé dirigeant de l'étude. L'escroc peut usurper l'identité d'un grand cabinet d'audit ou de conseil fiscal afin d'inspirer confiance. Il demande au service comptable d'effectuer **en urgence** un important virement, en insistant sur le caractère confidentiel de la transaction. Prise au dépourvu et pressée par son interlocuteur, la victime – en général salariée de l'étude et subordonnée à l'associé dont l'escroc se réclame – effectue le virement sans procéder aux vérifications usuelles **pourtant indispensables**.

La plus souvent, les escrocs demandent à leurs victimes de virer les fonds vers un compte ouvert à l'étranger. S'agissant des études notariales, les comptes visés par les escrocs sont tenus par la Caisse des Dépôts et Consignations (CDC), laquelle impose un délai de 48h incompressible pour valider l'ajout d'un nouveau bénéficiaire étranger. Dans ce cas, les escrocs proposent des RIB de comptes ouverts en France.

2. Le changement de RIB :

Les escrocs vont chercher à modifier ou substituer les RIB avec lesquels travaille l'étude :

- soit le **RIB de l'étude** elle-même, afin d'abuser un client acquéreur d'un bien immobilier, qui doit verser des fonds à l'étude.
- soit le **RIB d'un client** de l'étude, vendeur d'un bien immobilier, afin d'abuser l'étude lorsque celle-ci doit virer au client le produit de la vente du bien.

Les changements de RIB s'effectuent par **divers moyens** :

- par **piratage du réseau informatique** de l'étude (mail contenant une pièce jointe piégée ; clé USB piégée adressée à l'étude ou laissée à proximité, en espérant qu'un employé la branchera sur le réseau de l'étude, etc.) : les escrocs peuvent alors accéder aux serveurs de l'étude, identifier les clients acquéreurs ou vendeurs, et modifier les RIB qu'ils souhaitent.
- par **appel téléphonique** en usurpant l'identité d'un client et en manipulant un employé de l'étude.
- simplement par **envoi de mails** usurpant l'identité du client ou de l'étude et informant d'un changement de RIB, le nouveau RIB à utiliser étant celui des escrocs (souvent un PSP à l'étranger).

3. L'escroquerie au faux conseiller bancaire :

Comme de nombreux particuliers et professionnels, les études notariales peuvent être victimes des **escroqueries au faux conseiller bancaire.** L'escroc, par téléphone, se fera passer pour le conseiller bancaire de l'étude, invoquera une situation d'urgence (« des débits frauduleux ont été constatés sur le compte de l'étude ») et, au prétexte d'annuler les débits frauduleux, fera valider des paiements en sa faveur ou tentera de récupérer les identifiants bancaires de la société.

A noter que ces différentes attaques sont souvent menées **en fonction d'un calendrier précis** : veilles de week-end ou de jours fériés, congés scolaires, déplacements ou congés des responsables de l'étude.

Recommandations :

En amont :

- **Sensibiliser et former l'ensemble du personnel de l'étude,** et particulièrement ceux susceptibles d'être contactés par les escrocs (services comptables en premier lieu…).
- Au besoin, **réaliser des affiches** à disposer dans les bureaux des personnels les plus exposés.
- Prendre le temps de **vérifier les adresses de messagerie**. En général, les escrocs utilisent des adresses qui copient le plus possible les adresses de sociétés connues, en ne faisant varier qu'un ou deux caractères, ou un trait d'union, ou le nom de domaine final (.net au lieu de.fr).
- Mettre en place une **procédure de double vérification** des transactions **urgentes** ou de **montants élevés**, avec des contre-appels vers le donneur d'ordre supposé.
- **Ne pas rappeler les numéros de téléphone** indiqués dans les échanges de mail.
- **Sécuriser et mettre à jour systématiquement les systèmes d'information** (antivirus, firewalls…).
- **Rester discret sur les réseaux sociaux** : les informations qui y sont divulguées permettent aux escrocs de parfaire leur « couverture » ou leur scénario d'approche.

En cas de FOVI avéré :

- **Contacter au plus vite le chargé d'affaires de son établissement bancaire** afin qu'un rappel des fonds soit demandé auprès de la banque du bénéficiaire (cette opération n'est pas toujours possible).
- **Conserver l'ensemble des documents** : les échanges de mails avec leurs en-têtes détaillés, le cas échéant les fax, les relevés des numéros d'appel et/ou de fax, une copie du relevé d'identité bancaire fourni par l'escroc, éventuellement un enregistrement audio des appels téléphoniques.
- **Déposer plainte** en étant **le plus précis possible** : date et heure des faits, mode opératoire, nombre de virements opérés, montant exact des fonds virés, références complètes des comptes bancaires destinataires des fonds, numéros de téléphone et adresses mail complètes utilisés par les escrocs.
- Le cas échéant, faire déposer une **plainte auprès des autorités judiciaires du pays destinataire des fonds**, par le biais d'un **avocat local,** sauf si les fonds ont déjà été retournés par la banque d'origine. Dans certains cas, le dépôt de plainte peut constituer un préalable indispensable au gel des fonds.

Liens utiles :
- Guide de prévention contre les arnaques – Task Force nationale de lutte contre les arnaques : https://www.economie.gouv.fr/files/files/2022/Guide-TF-actualise-1907.pdf
- Ordre de virement des entreprises : 9 reflexes sécurité : https://www.lesclesdelabanque.com/entreprise/ordres-de-virement-des-entreprises-9-reflexes-securite/
- Module d'e-learning : Prévenir l'escroquerie au changement de coordonnées bancaires : https://www.lesclesdelabanque.com/entreprise/prevenir-escroquerie-aux-coordonnees-bancaires/