Décembre 2016

RISQUE D'USURPATION D'IDENTITÉ DE SOCIÉTÉ

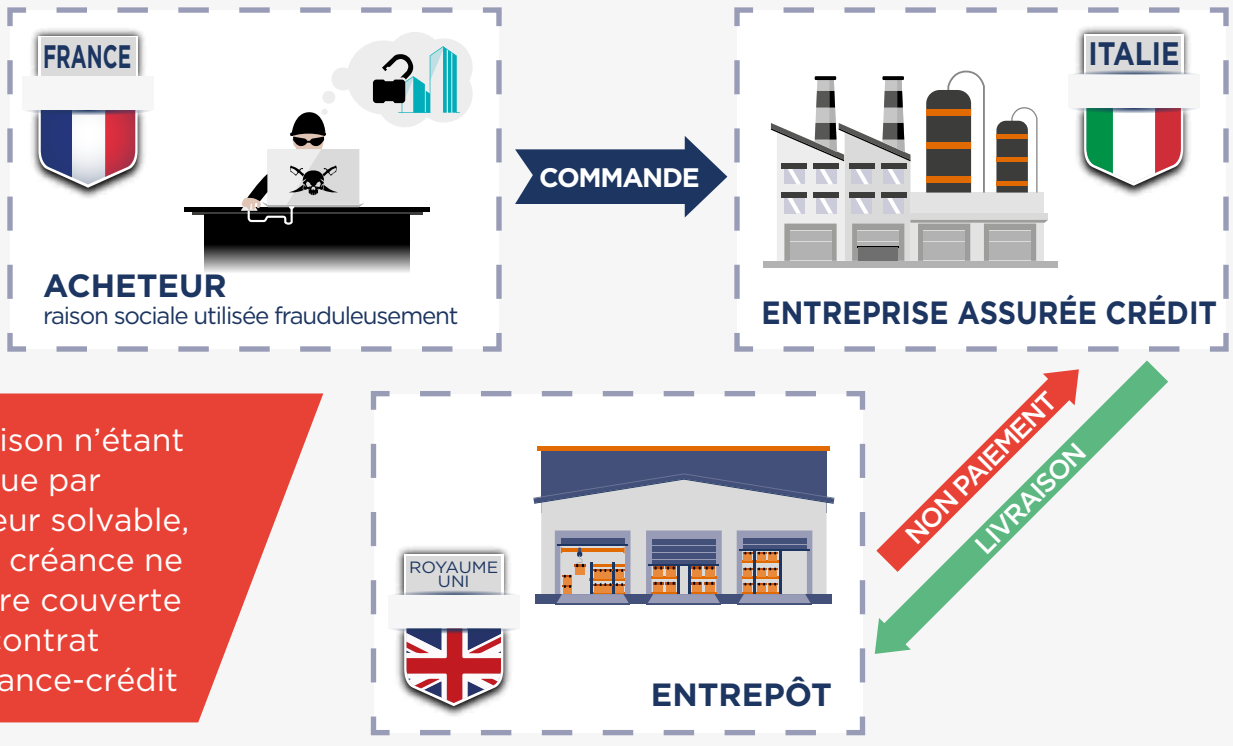
Les tentatives d'usurpations d'identité se multiplient sur le marché des échanges interentreprises. Son large spectre et sa nature évolutive obligent les entreprises à prendre des mesures visant à protéger leur identité et leur trésorerie contre ce fléau.

Etre confronté à une fausse identité d'entreprise, ou à l'utilisation illicite d'une raison sociale existante, peut vous mettre en situation de risque opérationnel important.

Ces dernières semaines, Coface a eu connaissance de plusieurs fraudes liées à l'usurpation d'identité et recommande une vigilance accrue.

Dans la pratique, les fraudeurs utilisent l'identité commerciale d'une vraie société, dont la réputation et le comportement de paiement sont plutôt bons, pour acheter des biens et des services auprès de nos clients / assurés crédit.
Le mécanisme de fraude auquel nous avons récemment été confrontés peut être représenté comme suit :

Exemple d'usurpation d'identité



La livraison n'étant pas reçue par l'acheteur solvable, aucune créance ne peut être couverte par le contrat d'assurance-crédit

Les fraudeurs agissent de façon plutôt bien organisée. Ils ouvrent des lignes téléphoniques, créent des adresses électroniques, falsifient des bons de commande, procèdent à des enregistrements auprès du registre du commerce, de façon à pouvoir ouvrir un compte client auprès d'une société. Il convient donc d'être vigilant lorsque vous recevez un bon de commande, en particulier s'il est émis depuis l'étranger par un nouveau client.

Il est en fait avéré qu'un faux bon de commande n'est jamais parfait. Cela vaut donc la peine de prendre un peu de temps pour faire certaines vérifications afin d'éviter de donner suite à une commande frauduleuse.

Lorsque votre service administration des ventes / commercial reçoit une commande, un problème évident peut être mis en lumière en vérifiant les points énumérés ci-dessous. Par conséquent, vous devez veiller :

• À comparer le logo de la société figurant sur son site Internet avec celui figurant sur la commande, car il peut s'avérer différent.

• À comparer le format d'adresse électronique (nom de la personne et de la société) de votre correspondant avec celui que vous pouvez trouver sur le site Internet (souvent à la rubrique « Contact »), car toutes les adresses électroniques d'une société ont généralement le même format. Toute différence doit être considérée comme suspecte (ex: david_smith@raison-sociale.fr devient d.smith@raison-sociale-service.com ou smith_david@nom-de-groupe.eu).

Faites particulièrement attention aux adresses électroniques génériques (ex : comptabilité@raison-sociale.com).

Les fraudeurs utilisent généralement le nom de personnes travaillant réellement au sein de la société.

• À comparer le format du numéro de téléphone (en particulier les 2 premiers chiffres).

• À vérifier si la société a des activités, une filiale ou un projet dans le pays où les produits doivent être livrés.

• À déceler d'éventuelles erreurs de syntaxe ou fautes d'orthographe dans le bon de commande, notamment dans les conditions particulières. Vous devez donc prêter attention à ce document et mettre en place des mesures internes pour contrôler sa validité.

• À vous demander si l'activité de ce client est compatible avec la vôtre.

Faites confiance, mais vérifiez : en cas de doute (bon de commande, modifications de coordonnées bancaires…), appelez toujours votre client pour confirmer et veillez à ce que vos chargés de compte comprennent l'importance de cette question.

Rappel : les cas d'hameçonnage (« phishing cases ») et de paiements effectués sur de faux comptes bancaires sont encore fréquents. Il est donc important de vérifier systématiquement toutes les demandes de modification (adresse, compte bancaire) auprès de votre partenaire.

FAX ET E-MAILS NE SONT PAS SÉCURISÉS

coface
FOR SAFER TRADE