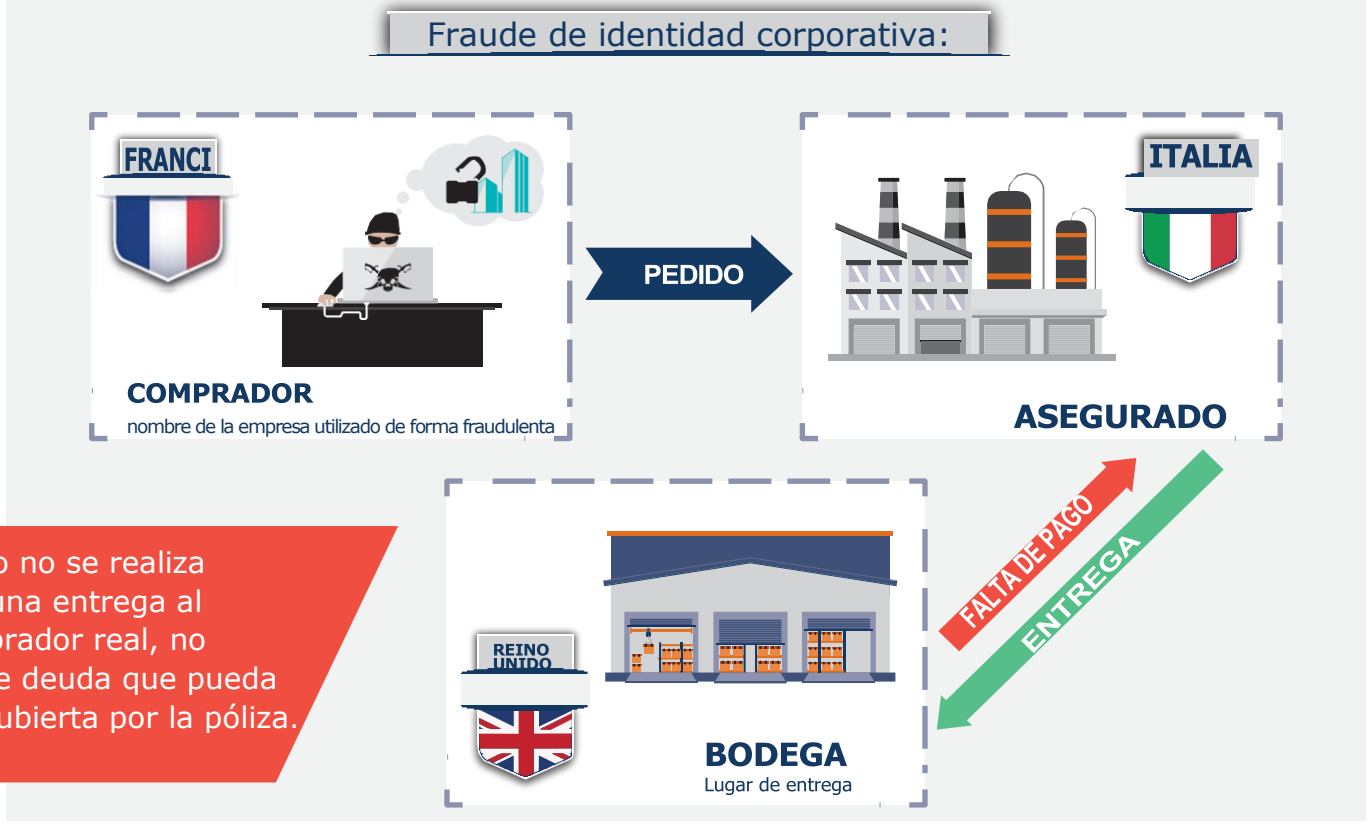
ALERTA SOBRE FRAUDE DE IDENTIDAD CORPORATIVA

El fraude de identidad corporativo es un "negocio en auge" en el mundo B-to-B. Su amplio alcance y naturaleza evolutiva hace que las empresas deben tomar acciones proactivas para proteger sus activos e identidad contra esta plaga.

Representa un riesgo operativo grave el uso de la identidad corporativa de una empresa por parte de un estafador para respaldar una actividad ilegal.
En las últimas semanas, Coface ha sido informado de varias estafas relacionadas con el robo de identidad y recomienda una mayor vigilancia.

En la práctica, los estafadores utilizan la identidad comercial de una empresa real, preferentemente con un buen historial de pagos y reputación, para adquirir bienes y servicios de nuestros clientes / asegurados
El reciente esquema de fraude al que nos hemos enfrentado se puede describir de la siguiente manera:

Fraude de identidad corporativa:



Como no se realiza ninguna entrega al comprador real, no existe deuda que pueda ser cubierta por la póliza.

Para operar, los estafadores están bastante bien organizados, abren líneas telefónicas, crean direcciones de correo electrónico, falsifican formularios de pedidos, compran certificados de incorporación y finanzas al registro comercial con el objetivo de abrir una cuenta de comprador en una empresa.
Esta es la razón por la que se deben tomar algunas precauciones al recibir un formulario de pedido, especialmente cuando proviene del extranjero y de un nuevo comprador.

De hecho, un formulario de pedido falso nunca resulta perfecto. Vale la pena dedicar unos minutos a verificarlos, a fin de detectar si éstos podrían ser fraudulentos.
Cuando su departamento de adquisiciones, compras o comercial reciba un formulario de pedido, es recomendable revisar la siguiente lista de verificación básica a fin de detectar alguna señal sospechosa que pudiera darnos indicios de que se trata de un fraude:

- Compare el logotipo de la empresa en el sitio web oficial con el del pedido, a veces puede ser diferente.
- Compare el formato de la dirección de correo electrónico (nombre de la persona y de la empresa) de su correspondencia con los que puedes encontrar en el sitio web (a menudo en el enlace de navegación "Contacto"). normalmente solo hay un formato para toda la empresa. Cualquier diferencia debe considerarse sospechosa (Ej. ana_smith@company.fr se convierte en a.smith@company-service.com o smith.a@company-group.eu)
  Los estafadores suelen utilizar nombres de personas que realmente trabajan para la empresa, pero con dominios un poco distintos para confundir.
- Tenga especial cuidado con las direcciones de correo electrónico genéricas, por ejemplo: contabilidad@empresa.com.
- Compare el número de teléfono proporcionado con los disponibles en la página web oficial, o en fuentes oficiales.
- Verificar si la empresa tiene una subsidiaria o un proyecto en el país donde solicitan entregar la mercadería.
- Los errores de sintaxis o errores ortográficos se pueden encontrar en el formulario de pedido y especialmente en las condiciones específicas. Por lo tanto, debe prestar atención a dicho documento y establecer medidas internas para verificar la validez del documento.
- Pregúntense si la actividad del comprador es compatible con la suya.
- Confíe, pero verifique: en caso de cambios en pedidos, dirección de entrega, cambio de datos bancarios, etc., siempre llame a su comprador para confirmar y asegúrese de que los cambios son reales.
- Como recordatorio, los casos de phishing y los pagos realizados en cuentas bancarias falsas siguen siendo comunes. Por lo tanto, siempre es importante confirmar todo tipo de solicitudes de cambio (dirección, cuenta bancaria) con su proveedor)

FAX Y LOS CORREOS ELECTRÓNICOS NO SON SEGUROS

coface
FOR TRADE