# Cómo Combatir el Fraude

## Señales de Alerta

### Para correos electrónicos, correspondencia, llamados telefónicos, transacciones y comunicaciones de sistemas

**¿Cómo sabe si el correo electrónico, llamado telefónico o correspondencia que Usted recibió solicitando información o dando instrucciones para una transacción son fraudulentos? Los engaños a la confianza que se basan en la psicología humana y otras tácticas de la ingeniería social tienen protagonismo en el intento de cometer fraude. Esté atento: reconocer engaños y hacer preguntas es el reflejo más efectivo para combatir el fraude.**

### ¿Ha notado?

- Lenguaje alarmista o exageradamente adulador
- Solicitudes de transacción abusivas o agresivas
- Cambios en el tono o en el comportamiento usual del cliente
- Sugerencias de pérdida de dinero si Usted no actúa
- Nombrar a funcionarios de alta jerarquía para acelerar la transacción

- Errores de gramática, sintaxis u ortografía en la redacción
- Instrucciones con un logo falso, a través de fax o enviadas por correo electrónico
- Contactos o detalles que no coinciden con los del banco
- Variaciones en la dirección de correo electrónico o cambios en el nombre del dominio

- Llamado del cliente/proveedor antes de poder realizar la verificación telefónica
- Cambios en el número del cliente/proveedor empleado para realizar la verificación telefónica
- El cliente/proveedor no se encuentra disponible a través de los canales oficiales
- El cliente/proveedor parece ansioso para realizar la transacción

- Los detalles de contacto del cliente/proveedor no están en nuestros registros
- Proveedores desconocidos o detalles de transacción alterados
- Pasos adicionales en el inicio de sesión o en ejecución de transacciones
- Instrucciones del sistema que "aparecen" misteriosamente

### ¿Le están solicitando que haga...?

- Recibir llamadas no solicitadas de contactos desconocidos
- Contactar supuestos clientes en números no habituales
- Dar una contraseña en un lugar que Usted no reconoce
- Aceptar detalles de contacto adjuntos o no confirmados
- Recibir o actuar bajo instrucciones no solicitadas
- Hacer clic en links inesperados, desconocidos o falsos

- Evitar procedimientos con razones convincentes
- Tratar con un beneficiario por primera vez o desconocido
- Brindar confirmación de pago SWIFT por correo electrónico
- Llevar a cabo instrucciones después de un cambio de perfil
- Realizar cambios en los pagos de manera inmediata y urgente
- Extraer casi todo o todo el saldo de la cuenta

- Aprobar una transacción desconocida o inusual
- Transferir fondos a causa de o antes de unas vacaciones prolongadas
- Transferir fondos hacia un paraíso fiscal
- Transferir una suma pequeña seguida de una suma grande a un beneficiario
- Transferir fondos a una jurisdicción alternativa

## ¿Qué hacer y qué no?

### Para dispositivos (smartphones, tablets, laptops y PCs)

**Para adoptar estas prácticas recomendadas, Usted puede necesitar involucrar a su departamento de IT. Esto puede requerir que deba llevar a cabo una evaluación de riesgo en cumplimiento con sus propios controles y evaluaciones.**

### Lo que debe hacer...

- ✓ Utilizar software antivirus, spyware o malware que se actualice automáticamente.
- ✓ Instalar aplicaciones o software de proveedores acreditados en los que Usted sepa que puede confiar.
- ✓ Habilite el bloqueador de pop-ups de su navegador de internet para evitar ataques de software maliciosos.
- ✓ Cada vez que termine de usar CitiDirect BE cierre la sesión y cierre el navegador de internet.
- ✓ Mantenga su Java plug-in siempre actualizado de tal manera que su software se ejecute sin problemas y de acuerdo a lo esperado.
- ✓ Proteja con contraseñas cualquier dispositivo que Usted utiliza para acceder a la plataforma CitiDirect BE.
- ✓ Sospeche de cualquier llamado telefónico no solicitado proveniente de una persona desconocida.
- ✓ Cuelgue la llamada si tiene dudas acerca de la misma, luego llame o envíe un correo electrónico a su contacto conocido en Citi.

### Lo que no debe hacer...

- x Utilizar su computadora sin antivirus, anti-spyware o software de detección de malware.
- x Instalar aplicaciones o software de fuentes o compañías desconocidas en las cuales Usted no confía.
- x Utilizar tecnología sin un bloqueador de pop-ups nativo o de terceros para defenderse contra malware.
- x Dejar la ventana de su navegador de internet abierta en dispositivos luego de haber finalizado la sesión de CitiDirect BE.
- x Utilizar un dispositivo o computadora sin la versión más reciente del Java plug-in.
- x Acceder a CitiDirect BE en cualquier dispositivo o tecnología que no se encuentren protegidos por contraseña.
- x Compartir su Desafío/Respuesta con cualquier persona (Citi no le pedirá que comparta esta información).
- x Hacer clic en cualquier hipervínculo inesperado de un correo electrónico.
- x Compartir pantallas de PC con personas no autorizadas.

## Riesgos y Controles

### Para cambios en los beneficiarios

**Reconocer el problema es clave para aplicar las mejores prácticas en soluciones. Estos consejos, cuando se aplican conjuntamente con sus propios procesos de control interno reducirán el riesgo asociado al cambio de los detalles de pago del beneficiario.**

#### Los problemas con los estafadores son que...

- Operan en todos los mercados, sectores, geografías.
- Trabajan de manera creativa y sofisticada.
- Hacen intentos para re-direccionar pagos.
- Buscan cambiar los detalles bancarios de los beneficiarios.
- Especulan con que Usted acepte logos falsificados.
- Intentan notificarle acerca de nuevos cambios bancarios.
- Se hacen pasar por nuevos oficiales de cuenta/técnicos del banco.
- Violan cuentas de correo electrónico de personal jerárquico para solicitar un pago.

#### Las maneras de reducir el riesgo de fraude son...

- Crear su propio perfil de cliente/proveedor/pagador.
- Validar de manera independiente todas las solicitudes de modificación que reciba.
- Confirmar las instrucciones por escrito con contactos conocidos.
- Nunca procesar acuerdos de solicitantes desconocidos.
- Verificar solamente a través de canales y contactos aprobados.
- Asegurarse que los procesos de pago del beneficiario sean sólidos.
- Estar siempre atento a solicitudes inusuales o que contienen señales de alerta.

## Mejores Prácticas

### Acciones para proteger su organización

- Si quiere **EJECUTAR** controles para reducir el riesgo de fraude.
  - » Valide las instrucciones de pago para cualquier beneficiario nuevo; la misma validación debe aplicarse a cualquier solicitud de cambio recibida a futuro.
- Si quiere **GESTIONAR** transacciones de alto valor o alto riesgo
  - » Establezca niveles de aprobación adicionales bajo la lógica maker/checker de CitiDirect BE.
- Si quiere **REDUCIR** el riesgo transaccional en todo el negocio
  - » Segregue los roles para actividades sensibles o de alto riesgo.
- Si quiere **COMPRENDER** mejor la ingeniería social
  - » Promueva la capacitación sobre amenazas cibernéticas/conciencia sobre fraude.
- Si quiere saber cómo **MONITOREAR** la actividad del usuario
  - » Revise periódicamente los informes y tableros de control y lleve a cabo frecuentes auditorías sobre los usuarios.
- Complete la capacitación que Citi le brinda acerca del Fraude de Ingeniería Social disponible en **http://www.citibank.com/tts/sa/emea_marketing/training/index.html**

**SI USTED ES VICTIMA DE UN ATAQUE, CONTACTE A SU SECURITY MANAGER Y A SU CONTACTO HABITUAL DE CITI. CITI TIENE UN SERVICIO DE INVESTIGACION DE FRAUDE QUE ESTÁ COMPLETAMENTE CAPACITADO PARA INVESTIGAR Y TRATAR CON ATAQUES DE FRAUDE.**

1462072 09/16