FAQ's

1 What type of information security does BUSA Servicing Inc. offer for transactions or inquiries available on the Internet?
A: BUSA Servicing Inc. utilizes many lines of defense - including encryption, session time-outs and firewalls.

2. What is a fraudulent/spoof email?
A: A fraudulent (a.k.a. spoofing, imposter, or phishing) email is one that has been forged so it looks like a legitimate e-mail from a particular organization (such as BUSA Servicing Inc.). Its goal is to trick you into providing sensitive personal information that can be used for identity theft.

3. How do I spot a fraudulent/spoof email and how do I report it?
A: It is often difficult to detect a fraudulent email. That is because the email address of the sender may seem genuine (such as support@ccbusa.com), as do the design and graphics, but there are some telltale signs to be aware of. To bait you, emails may allude to an urgent or threatening matter concerning your account. Fraudulent emails often try to extract personal information from you such as passwords, PINs, credit card CVV codes, Social Security Numbers or bank account information. Spoof emails may:

- Lure you into providing sensitive information on the spot (e.g., by replying to an email)
- Include embedded links to a site that will ask you to disclose personal data
- Convey a sense of urgency
- Have obvious spelling errors

If you suspect that you have received a fraudulent e-mail message, please forward it to us. Do not change or retype the subject line, as this makes it more difficult to properly investigate. After forwarding the email, you should delete it from your inbox. Forward suspicious emails to: spoof@citicorp.com or Call 1-888-285-9696.

4. How can I be sure that I'm dealing with BUSA Servicing Inc. and not an imposter?

- A: You can tell that you're dealing with BUSA Servicing Inc. because:
- BUSA Servicing Inc. will never send you an email asking for your passwords, credit card numbers, or other sensitive information
- If we request information from you, BUSA Servicing Inc. will always direct you back to the BUSA Servicing Inc. site using secure links. If you are required to enter personal information to perform a transaction, such requests will be performed on a secure site. Secure sites have a padlock icon at the bottom of the screen. To confirm the security of a BUSA Servicing Inc. site, click on the padlock icon and read the pop-up security certificate. If the site is a secure BUSA Servicing Inc. site, the section stating "Issued to" will have a URL ending in "BUSAServicingInc.com."

Preguntas Frecuentes

1. ¿Qué tipo de seguridad ofrece BUSA Servicing Inc. al realizar operaciones o consultas a través del Internet?
R: BUSA Servicing Inc. incorpora diferentes niveles de seguridad que incluyen encriptación, límites al tiempo de inactividad, y software de barrera de protección (firewall).

2. ¿Qué es un correo electrónico fraudulento?
R: Un correo electrónico fraudulento (también conocido como correo engañoso, impostor, robo de identidad, etc.), es un correo electrónico que se ha falsificado para que tenga la apariencia de un correo electrónico legítimo de una organización en particular (tal como BUSA Servicing Inc.). El objetivo de esos correos fraudulentos es engañarlo para obtener información personal y confidencial que se pueda usar para el robo de identidad.

3. ¿Cómo puedo determinar si un correo electrónico es fraudulento y como lo reporto?
R: A menudo es difícil detectar un correo electrónico fraudulento. Esto es porque la dirección del correo electrónico del remitente puede parecer legitima (por ejemplo; support@ccbusa.com), Así como los formatos e imágenes en el correo. Pero aun así, existen indicadores útiles para reconocer correos y sitios fraudulentos. Con el propósito de confundirle, los correos fraudulentos podrán expresar un tono de urgencia o amenaza referente a su cuenta. Estos correos intentan obtener información personal y confidencial tales como contraseñas, Numero de PIN, código CVV de la tarjeta de crédito, número de seguro social, o información de su cuenta bancaria. Los correos fraudulentos podrían:

- Conllevarlo a proporcionar informaciÃ³n confidencial en el mismo momento (Por ejemplo, dando repuesta al correo).
- Incluir enlaces incorporados a un sitio que le solicitará proporcione sus datos personales.
- Usan un tono de urgencia.
- Contienen evidentes errores ortográficos.

Si usted sospecha que ha recibido un correo electrónico fraudulento, por favor reenvíenos dicho correo. No cambie nada en el correo (incluyendo la línea del asunto) por la razón que cualquier cambio podrá hacer difícil investigar el asunto adecuadamente. Después de enviarnos el correo, elimínelo de su buzón de entrada. Reenvíe correos sospechosos a: spoof@citicorp.com o llame al 1-888-285-9696.

4. ¿Cómo puedo estar seguro de que estoy tratando con BUSA Servicing Inc. y no con un impostor?
R: Usted puede saber que está tratando con BUSA Servicing Inc. porque:

- BUSA Servicing Inc. nunca le enviará un correo electrónico pidiéndole sus contraseñas, sus números de tarjetas de crédito u otra información confidencial.
- Si le solicitamos información, BUSA Servicing Inc. siempre le dirigirá a que regrese a la página de BUSA Servicing Inc. usando enlaces de internet seguros. Si se requiere información personal para procesar una transacción, esta se solicitará por medio de un sitio seguro de internet. Sitios seguros muestran una imagen de un candado en la parte inferior de la pantalla. Para confirmar la seguridad de un sitio de BUSA Servicing Inc., haga clic en la imagen del candado y verifique el "pop-up" del certificado de seguridad. El sitio de BUSA Servicing Inc. es seguro si la parte donde dice "Issued to" (expedido a) contiene un URL con terminación " BUSAServicingInc.com."