Information for your safety

We have established an effective control to protect the confidentiality, security and integrity of all customer information and ensure security of online transactions. Protecting the privacy and confidentiality of communications is our highest priority.

Please note that you must exercise the same care and caution when using your online account with us. Below are some guidelines that can help protect your information and provide a safer online experience.

PC Security

Keep your PC safe. Use antivirus software and anti-spyware. Use this program to perform frequent checks to detect and remove programs that could be harmful to your computer or could obtain personal information.

Use the latest version of the browser. Keep your browser up to date will help ensure you have the latest security updates for your browser. When you use online services, we suggest using the recommended browser for this service.

Make sure you have a firewall installed and enabled on your computer. A personal firewall can help prevent unauthorized users from accessing your computer.

Do not click on suspicious links in pop-ups or emails, even from people you know. May be tricks to install spyware and steal personal or financial information.

We suggest you do not go into your online account from computers that are not controlled by you or your business. For example, do not log in from computers in libraries, hotels or any other public place.

Protecting your Account Information

When you originate a payments online, verify the safety symbols for online payments that look like a lock icon on the status bar of the browser, also verify the presence of an "s" after "http" in the URL, or the expression " Secure Sockets Layer (SSL). " These are certain signs that you're browsing in a secure

page for transmitting personal information.

Be suspicious of any connection or communication written information about your account. Do not provide such information, unless you who initiated the conversation.

Carefully check boxes on a form online before pre-fill your payment card information. If you do not uncheck the boxes can accept terms and conditions under which you are not interested.

Monitor the status of your card account is regularly and notify any suspicious or unauthorized charges.

Choose your password carefully and avoid easily guessed passwords related to your family, friends, pets, important dates, etc. Use symbols and numbers that make your unique password. Always keep your password and security question secret.

Information that reveals your identity can easily be subtracted in the virtual world as FICO. It is important to follow the instructions to destroy new PIN numbers and cards expired. You should also consider using a shredder to destroy personal documents with layers and sensitive. It is convenient to store the documents in a closed and secure.

Use alerts to stay current on your account activity.

It is important to completely disconnect from your online session, close the window where he was made the transaction cannot close the session. If your computer is infected with a Trojan, the session can be hijacked by a criminal and financial transactions could be made without your knowledge.

It is also recommended to disconnect from the internet if you do not plan to use it.

Memorize your password. Never write your password information or security question.

Never give out your account information during calls, chat sessions or verbally, without knowing who they are and why they want the information.

If you receive a call that seems suspicious, write down the details and call the phone number printed on the back of your card.

Contact

It is essential you inform us as soon as possible if:

suspects or discovers that someone knows your password or security question

suspects or discovers a fraudulent transaction.

The best way to contact us is through the telephone number printed on the back of your card or by clicking here. Please do not hesitate to contact us with any questions you have.