BANCO INTERNACIONAL DE COSTA RICA

If you use BICSA's online banking, mobile banking, or other internet banking services as an individual consumer or as a business, you will be interested to know that BICSA is in compliance with the Federal Financial Institutions Examination Council (FFIEC) requirements and standards in order to make all of your personal and business accounts more secure. New supervisory guidance from the Federal Financial Institutions Examination Council (FFIEC) is intended to help banks strengthen their vigilance to assure that your accounts and online transactions are properly secured.

Account Authentication and Online Banking
BICSA uses Multi-factor authentication and layered security to help assure safe internet transactions for all our customers.

Authentication: Understand the Factors
The authentication process is of vital importance to verify that YOU, and not someone who has stolen your personal identity or hijacked your corporate account, is conducting your online transactions. Authentication usually involves one or more basic factors:

- something the user KNOWS (such as a password or PIN)
- something the user HAS (such as a Token)

BICSA's Multi-factor authentication uses more than one method, and is a much stronger fraud deterrent.

Internal Assessments at BICSA
The new supervisory guidance offers ways BICSA can look for anomalies that could indicate fraud. BICSA has conducted a comprehensive risk-assessment of its current methods with regards to the following:

- changes in the internal and external threat environment
- changes in the customer base adopting electronic banking
- changes in the customer functionality offered through electronic banking, and
- actual incidents of security breaches, identity theft, or fraud experienced by the institution or the industry.

Whenever an increased risk to your transaction security may warrant it, BICSA will be able to conduct additional verification procedures or layers of control such as:

- utilizing call backs (voice) verification
- employing customer verification procedures
- analyzing banking transactions to identify suspicious patterns
- establishing dollar limits that require manual intervention to exceed a preset limit

Layered Security for Increased Safety
Layered security is characterized by the use of different controls at different points in a transaction process, so that a weakness in one control area is compensated by strength in another control area.

Layered security can substantially strengthen the overall security of online transactions by protecting sensitive customer information, preventing identity theft, and reducing account takeovers with their resulting financial losses.

Added layers of security allow your bank to authenticate customers and detect and respond to suspicious activity related to initial login and then reconfirm this authentication when further transactions involve transfers of funds or higher risk actions.

Examples of Layered Security for Businesses
For business accounts, layered security can include enhanced controls for system administrators who are granted privileges to set up or change system configurations, and control access privileges and application functions or limitations for their own staff and users. Added layers can include:

- fraud detection and monitoring systems that include consideration of your transaction history and behavior
- dual customer authorization through different access devices
- out-of-band verifications for certain transactions
- "Positive Pay" debit blocks or other techniques that limit transactions
- transaction value thresholds that restrict the number or amount of transactions for a set time frame
- Internet Protocol (IP) reputation-based tools
- policies and procedures for addressing customer devices that have been potentially compromised, or for detecting customers who may be facilitating fraud
- account maintenance controls over activities performed online or through customer service channels.

Identity Theft

Account takeovers have increased every year, representing losses of hundreds of millions of dollars. When an account takeover occurs, legitimate login credentials are stolen by computer hackers, and fraudulent transfers (ACH or Wire Transfers) are completed before the business account owner knows what happened.

Identity theft occurs when an unscrupulous person (Criminal) assumes the identity in some form of an innocent victim. Despite the efforts of law enforcement, Identity Theft is becoming more sophisticated and the numbers of new innocent victims is growing alarmingly thus sometimes suffering actual losses. If the crime is not detected early, people may suffer prolonged periods of time cleaning up the damages to their reputation and credit rating. The evolution of Identity Theft includes the spread of fraudulent "phishing" e-mails. These are unsolicited e-mails purportedly from a legitimate source, perhaps a bank, utility company, well-known merchants, your internet service provider or even a trusted government agency such as the Federal Reserve Bank, the FDIC or other regulatory agency attempting to trick you into divulging personal information. Identity Theft can affect consumers in many ways, but there are

also many ways to keep your identity from being “hijacked” and to assist you if you have been a victim of it:

- Protect your Social Security Number (SSN), Cedula de Identidad, credit and debit cards, PINs (Personal Identification Numbers), Passwords and other personal information.
- Protect your incoming and outgoing mail.
- Keep you financial trash “clean”, shred sensitive financial documents instead of discarding them in the trash.
- Keep a close watch on your bank account statements and credit bills.
- Exercise your new rights under FACTA to review your credit record and report fraudulent activity.

Customer Vigilance!
Knowing how fraudsters may try to trick you and understanding the risks is critical to safe online banking. You can take further steps to protect yourself and make your computer safer by installing and regularly updating:

- anti-virus software
- anti-malware programs
- firewalls on your computer
- operating system patches and updates

Additional steps include:

- create strong complex passwords that contain both CAPITAL and small letters, numbers and any allowed special characters
- if you think you may have visited a website with malware or if you think your computer may be infected with a virus, do not access your online banking or other sensitive logins until you have scanned your computer and know it is clean and virus free.

Understand the Risks
FFIEC studies show significant increase in cyber threats. Not only do fraudsters continue to deploy more sophisticated methods to compromise security measures, they now manufacture computer hacking kits to sell illegally to less experienced fraudsters.

Web Browser Requirements

You will need to have installed:

- Internet Explorer version 9 or higher
- Google Chrome 42 or higher
- Safari 5.1 or higher
- Mozilla Firefox ESR 38 or higher

Recommendations for Business Accounts

- conduct periodic assessments of internal controls
- use layered security for system administrators
- initiate enhanced controls over high-dollar transactions
- provide increased levels of security as transaction risk increase

External Link Disclaimer
BICSA has no control over information at any site hyperlinked to or from this site. BICSA makes no representation concerning and is not responsible for the quality, content, nature, or reliability of any hyper linked site and is providing this hyperlink to you only as convenience. The Privacy and security policies of the hyperlinked site may differ from those of BICSA. The inclusion of any hyperlinked site, in no event shall BICSA be responsible for your use of a hyperlink.

What BICSA does with YOUR Information
Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share and protect your personal information. Please read this notice carefully to understand what we do.

To protect your personal information from unauthorized access and use, we use security measures as previously mentioned that include computer safeguards and secured files and buildings.

BICSA's employees are bound by our Code of Ethics and policies to access consumer information only for legitimate business purposes and to keep information about you confidential.

The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number or Cedula de Identidad
- Account balances and transaction history
- Payment history and credit history

If you are a *new* customer, we can begin sharing your information 30 days from the date we sent this notice. When you are *no longer* our customer, we may continue to share your information as described in this notice.

However, you can contact us at any time to limit our sharing.

If You Have Suspicions
If you notice suspicious activity within your account or experience a security related event (such as loss of token, compromised PIN or Password, known or suspected infection of computer or network by viruses or malware, etc.) please contact your bank immediately, and you will be quickly and courteously directed to a customer service representative who can assist you with these matters.

If You Have Questions
You may contact us at:

- Customer Service: (507) 208-9500
- Email: servicioalcliente@bicsa.com

Login and Logout Messages:

- **Log In Message**:

- **Log off Message:**