Customer Security Awareness Education
For Both Retail and Business Customers

For most of us the Internet has become a basic part of daily life. As the comfort level with the internet continues to grow so does doing other types of business online. Millions of consumers today are doing some or all of their banking online.

It's convenient and efficient. You can access your account and make banking transactions at anytime from anywhere you have an Internet connection. Investar Bank offers Online Banking and Mobile Banking as a free service.

Through our Online Banking service, you can manage eligible accounts from your home or office computer or internet enabled mobile device. Online Banking can be used to conduct any of the following "On-line Financial Services":

A. To receive and download balance and transaction information for INVESTAR BANK accounts

B. To transfer funds between any authorized Accounts

C. To export account information into a formatted file. This file will be downloaded onto your computer where it will be available for import into a personal financial management software program

D. To initiate a stop payment on a check

E. To receive your monthly statements online

F. To apply for products and services

G. To pay bills electronically from a Deposit Account

H. To receive e-mail from and transmit e-mail to the Bank

* Please review the full Online Banking Disclosure for complete list of user guidelines.

With the use of the internet and Online Banking increasing so does internet fraud. Investar Bank has preventative controls in place to help deter Online Banking fraud. Online Banking users should review the below controls as well as the **Basic Online Security Practices for Both Retail and Business Customers** for more information on fraud prevention education. Investar Bank also encourages account holders to review security education resources that help customers keep abreast of new and emerging issues, such as online security magazines and security vendor websites.

Education

Examples of Deceptive Ways Criminals Contact Account Holders

- The FDIC does **not** directly contact bank customers (especially related to ACH and Wire transactions, account suspension, or security alerts), nor does the FDIC request bank customers to install software upgrades. Such messages should be treated as fraudulent and the account holder should permanently delete them and not click on any links. User should also keep in mind; Investar Bank will not contact a customer on an unsolicited basis and will never ask you to provide them with Online Banking credentials such as the password, security answers and questions or secure token information.
- Messages or inquiries from the Internal Revenue Service, Better Business Bureau, NACHA, and almost any other organization asking the customer to install software, provide account information or access credentials is probably fraudulent and should be verified before any files are opened, software is installed, or information is provided.
- Phone calls and text messages requesting sensitive information are likely fraudulent. If in doubt, account holders should contact the organization at the phone number the customer obtained from a different source (such as the number they have on file, that is on their most recent statement, or that is from the organization's website). Account holders should not call phone numbers (even with local prefixes) that are listed in the suspicious email or text message.

Common Security Threats to your personal device may include:

- Phishing
- Spyware
- Malware

Please see **Basic Online Security Practices for Both Retail and Business Customers** for more tips on how online banking users can safe guard their personal banking information against these threats.

Fraud Detected??

CONSUMER PROTECTION – REGULATION E

Regulation E provides rules for error resolution and unauthorized transactions for electronic fund transfers, which includes most transactions processed online. In addition, it establishes limits to your financial liability for unauthorized electronic fund transfers. These limits, however, are directly related to the timeliness of your detection and reporting of issues to Investar Bank. It is for this reason that we encourage you to immediately review periodic account statements and to regularly monitor your account activity online.

The "Electronic Fund Transfers" disclosure provided to you at the time of account opening provides detailed information. We will provide to you, upon request, a free printed copy of this disclosure.

In the event suspicious account activity has occurred or information security –related events have been experienced please contact your local branch or contact Investar Bank directly at customerservice@investarbank.com or you can reach us at 1-866-604-2006

Sign on and General Controls

Investar Bank's online banking service is equipped with features that can help safeguard your sensitive personal account information:

Sign on restriction. Public or unsecured computers (for example, an Internet café or library) should not be used for accessing Online Banking.
Dedicated computer. An FBI recommended best practice is to suggest that company users dedicate a computer solely for financial transactions (e.g., no web browsing, emails, or social media).
Secure sign on registration. Customers should register their computers so they will not be required to answer the challenge questions on every login.
Password requirements. Online Banking uses strong password controls that require customers to use a combination of special characters, letters, and/or numbers. Passwords cannot be the same as the associated user ID or be one of X (configurable by your financial organization) previously used passwords. Passwords may be set to expire periodically.
Last sign on date and sign on attempts. The Online Banking Welcome page shows customers the last day and time (Eastern Time) they signed on. Customers should confirm this each time they sign on. Customers are allowed three unsuccessful sign on attempts before their account is locked and access is prevented
Inactivity timeout. Online Banking automatically signs customers off after 20 minutes of inactivity.
Account nicknames. Account numbers should not be used for account nicknames.
Secure tokens. Use of secure tokens is highly recommended at sign on.
Antivirus software and operating systems. Customers should keep their antivirus software and operating systems up-to-date.

Business Banking General Controls

Investar Bank encourages commercial users to evaluate each user role, limits and accessibility assigned to users. We also encourage commercial Online Banking customers to perform a risk assessment and evaluate controls periodically as it relates to their Online Banking access. We also encourage all business customers to develop an incident response plan and applicability of laws and regulations to business owners to safeguard information.

Additionally, Business account holders should be aware of their exposure to electronic theft. In particularly, corporate account takeovers and cyber thieves, exposure risks, security measures, beneifts of a risk assessment, insurance coverage needs related to electronic thefts and

User Roles and Entitlements

Service entitlements. Online Banking supports customer level entitlements for all services allowing Investar Bank to establish our own risk review process before allowing access to a feature.
Separation of duties. Customers should assign roles and use account entitlements to separate duties in a company. For instance, one user can enter an ACH or Wire transaction and another can transmit it.
Limit approvers. Role-based access can be used to limit the number of users with approval authority.

Alerts

Mandatory alerts. Online Banking supports the following mandatory alerts for all Online Banking users. An alert is automatically sent to customers in particular:

A password is changed.
An e-mail address is changed.
Failed Transfers (Internal and external).
Transfer Completed (Internal and external).

ACH (optional). An alert can be sent to customers when:
An ACH template has been added, edited, or deleted.
An ACH transfer is pending approval.

Wire (optional). An alert can be sent to customers when:
A wire transfer template has been added, edited, or deleted.
A wire transfer is pending approval.

Multiple Approvals

ACH. Multiple approvals can be required to send an ACH transaction. These can be set by Investar Bank or by a user at the company who has the Administration role
Wire. Multiple approvals can be required to send a wire. These can be set by Investar Bank or by a user at the company who has the Administration role.
Funds Transfer. Multiple approvals can be required to enter a funds transfer including external transfers. These can be set by Investar Bank or by a user at the company who has the Administration role.
File Transfer. Multiple approvals can be required for customers to send Files to Investar Bank including NACHA files. These can be set by Investar Bank or by a user at the company who has the Administration role.

History and Audit Information

Transfer history. History reports are available for ACH, Wire and Funds Transfer. Customers should review this information regularly.

Payment and Transfer Service Best Practices

ACH. The following action can be taken for ACH:

Prenotes. Financial organizations should recommend using prenote for new transactions.
NACHA guidelines. Investar Bank reviews their standard risk approval process for ACH activity per NACHA guidelines.

Wire. The following action can be taken for Wire:

Security PIN. Investar Bank uses the free form wire security PIN feature.
Wire review. Investar Bank reviews Wires in Online Banking before uploading wire files into our wire system.

Funds Verification

Balance check. Online Banking supports Funds Verification for out-going funds.

Resources for Business Account Holders

Additionally, Business account holders should be aware of their exposure to electronic theft. In particularly, corporate account takeovers and cyber thieves, exposure risks, security measures, benefits of a risk assessment, and insurance coverage needs related to electronic thefts. Below are resources available on these topics:

1. The Better Business Bureau's website on Data Security Made Simpler: http://www.bbb.org/data-security;
2. The Small Business Administration's (SBA) website on Protecting and Securing Customer Information: http://community.sba.gov/community/blogs/community-blogs/business-law-advisor/how-small-businesses-can-protect-and-secure-customer-information;
3. The Federal Trade Commission's (FTC) interactive business guide for protecting data: http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html;
4. The National Institute of Standards and Technology's (NIST) Fundamentals of Information Security for Small Businesses: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf;
5. The jointly issued "Fraud Advisory for Businesses: Corporate Account Takeover" from the U.S. Secret Service, FBI, IC3, and FS-ISAC available on the IC3 website (http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf) or the FS-ISAC website (http://www.fsisac.com/files/public/db/p265.pdf); and
6. NACHA – The Electronic Payments Association's website has numerous articles regarding Corporate Account Takeover for both financial institutions and banking customers: http://www.nacha.org/c/Corporate_Account_Takeover_Resource_Center.cfm