IMPORTANT FACTS ABOUT ONLINE BANKING AND ACCOUNT AUTHENTICATION FOR ONLINE BUSINESS TRANSACTIONS

If you use online or mobile banking for your business, you want to be assured that effective safeguards are in place to make your accounts more secure. Due to recent regulations, the Federal Financial Institutions Examination Council (FFIEC) is providing guidance to banks to increase their vigilance for business and consumer accounts.

Online security includes several factors and measures beginning with the authentication process, which is used to confirm that it is you, and not someone who has stolen your identity. At Bank of Guam these factors and measures include:

- PASSWORD PROTECTION
  - Your password is the first line of defense and is a unique identifier. Your password is issued to you for security purposes. It is confidential and should not be disclosed to third parties. You are responsible for safekeeping your password information.
- MULTI-FACTOR AUTHENTICATION
  - This form of identity verification provides added security by requiring multiple forms of identification, such as something you know (your challenge questions).
- LAYERED SECURITY
  - Layered security is described by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of the additional control. Layered security may help reduce account takeovers and the resulting financial losses by allowing Bank of Guam to authenticate its customers and detect and respond to suspicious activity related to initial login and then to reconfirm this authentication when further transactions involve the transfer of funds to other parties. For business accounts, layered security might often include enhanced controls for system administrators who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations and/or limitations.
- ENCRYPTION
  - Once online, your transactions and personal information are secured through encrypted transmission. Your information encrypted transmission is readable by only you and the Bank through a SSL Certificate with server-gated cryptography (SGC) that automatically steps up protection to 128 or 256-bit encryption for over 99.9% of Internet users. Protection can be seen by the green address bar which also verifies our identity.
- PRIVACY POLICIES
  - Bank privacy policies protecting your personal information are stringent. Your confidential information is treated with the utmost care.

ENHANCED CONTROLS

Not every online transaction poses the same level of risk, therefore more robust controls should be implemented as the risk level of the transaction increases. Generally online business transactions have a higher frequency and dollar amount than consumer transactions, therefore they pose an increased level of risk to the institution and its customer. Enhanced controls, preventive and detective, should be designed to exceed the controls applicable to routine customer users. For instance, these added controls over administrative access and functions can effectively reduce money transfer fraud.

INTERNAL ASSESSMENTS

There are also a number of measures taken internally to look for indications of fraud. Our main priority is to ensure that the authentication process used for a particular transaction is suitable for the transaction's level of risk. We are continuously conducting risk assessments of our methods and systems as recommended by regulatory guidelines. These assessments take into consideration changing internal and external threats, changes in technology and electronic banking as well as actual incidences of security breaches or fraud experienced within the industry or by our Bank.

When transactions are deemed as higher-risk transactions, we may use additional verification procedures or layers of control, including:

- Dual customer authorization for higher risk functions
- Fraud detection and monitoring which includes consideration of customer history and behavior. For instance, this would entail flagging a transaction in which a customer who normally pays $40,000 a month to five vendors suddenly pays $100,000 to a new vendor
- Out-of-band authentication and verification for transactions. Calling customers on designated numbers for verification or email approval
- Establishing parameters for transaction value, daily number of transactions, as well as appropriate time-of-day restrictions. If a preset dollar limit is exceeded, the Bank will intervene in order to complete the transaction
- Internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities
- Policies and procedures for addressing a customer's device identified as potentially compromised and customers who may be facilitating fraud
- Account maintenance controls over activities performed by customers either online or through customer service channels

RECOMMENDATIONS FOR BUSINESS ACCOUNTS

It is also highly encouraged that you are aware of your normal business activities so that you can more easily identify any authorized activities on your account. The following measures are recommended for business account holders:

- Conduct periodic assessments of your internal controls
- Use enhanced controls for high-dollar transactions and other high-risk transactions
- Use layered security for your system administrators

REG "E"

Banks follow specific rules for electronic banking transactions issued by the Federal Reserve Board. These rules, known as Regulation E (Reg E), pertain to a variety of situations involving electronic transactions. "Reg E" gives the individual consumer, a natural person, certain protections from unauthorized online banking transaction according to how soon they report them. In general, these protections are extended to consumers and consumer accounts which have been established primarily for personal, family, or household purposes.

CUSTOMER AWARENESS

Understanding these fraud risks and effective techniques you can use to mitigate those risks are vital steps in protecting yourself online. You can make your computer safer by installing and updating regularly your

- Anti-virus software
- Anti-malware programs
- Firewalls on your computer
- Operating system patches and updates

CONTACT US

If you notice any suspicious activity on your account or experience security related events (such as a phishing email from someone purporting to be from Bank of Guam), contact Bank of Guam immediately at (671) 472-5300 or (671) 472-5284 for assistance.