Customer Identity Authentication & Information Protection Awareness

Dear Customer:

MUFG Bank (Europe) N.V. is dedicated to protecting your company information you provide us and doing its best in preventing unauthorized access to your accounts. This Communication describes what we do in this regard and gives you the information you need to play your part in protecting yourself from identity theft and financial fraud.

The delivery of this information is highly recommended practice for banks in which you are receiving for informational purposes only. No action is required on your part other than carefully reviewing it and taking those actions you believe appropriate to protect yourself.

Should you find anything suspicious of fraudulent activity involving your account, we ask that you contact your Relationship Manager immediately.

Truly yours,

MUFG Bank (Europe) N.V.

Customer Identity Authentication & Information Protection Awareness

Identity theft and account or other financial frauds are serious events. These generally involve someone getting information about you and/or your accounts and using that information to impersonate you so they can withdraw funds from your account – or incur debts that you will be asked to repay. This communication describes what we do in this regards and gives you the information you need to play your part in protecting yourself from identity theft and financial fraud.

Customer Access Authentication

A bank that gives its customers remote access to an account (especially through the internet) needs to ensure those customers or their employees are who they say they are. The process by which this fraud is reduced is called customer authentication. Banks use a number of methods to authenticate a customer's identity, with most currently using one or more of the following: passwords, personal identification numbers (PINs) and digital certificates, etc. These methods involve something the customer knows (e.g., password, PIN).

What we do to protect you…

Encryption. We use a 2048-bit encryption supporting browser to access your account. Our encryption tools are some of the strongest available for commercial use.

User ID and Password. We **never** ask for your PIN or Password to help you. These are for you to securely access you information and accounts.

Firewalls. Our computers are protected by strong firewall systems that prevent unauthorized access to your information and accounts. We use them to prevent information and account security problems.

Timeouts. Your online sessions will automatically end-or "time out" – after a certain period of inactivity. To continue, you'll have to log into the system again.

MUFG Bank (Europe) Online Banking

Measures to follow when using MUFG Bank (Europe) Online Banking:

441. Keep your RSA token in secure place.

442. Only supply your sign-on credentials during sign-on and when confirming payment confirmations. Any requests for sign-on credentials outside of those may indicate malware is present on your PC.

443. Never share your RSA token or tell anyone your PIN. Please note that the Bank will **never** ask you to provide your RSA token credentials.

444. Confirm all payment instructions received via email by contacting the sender through some other method of communications such as phone call-back.

445. Check the last login date and time whenever you login to determine if there have been any suspicious or unauthorized logins.

446. Always logoff MUFG Bank (Europe) online banking when finished.

447. Use the MUFG Bank (Europe) online banking functionality that allows you to set limits on transactions and daily cumulative totals. You can place amount limits on your entire company. Your accounts, and on individual users.

448. Verify all payments as soon as they appear on processed payment lists.

449. Have your company's Administrator users verify all user activity through the use of the user activity report.

450. Always specify at least one approver for each transaction. The transactions approver should be a second user, and the approver should use a different PC than the creator of the transaction.

Reporting Suspicious Activity

If you suspect identity theft, see suspicious activity in your account(s) or receive a suspicious call, e-mail or letter supposedly from our Bank regarding your account, please contact your relationship manager.

We recommend business and commercial clients to implement controls and sound security practices to prevent unauthorized transactions. In addition, periodic assessment of the fraud risk must be performed to evaluate the effectiveness of those client implemented fraud prevention controls.

Helpful Tips

What you can do to protect your account and financial information…

- Change passwords often to maximize protection. Create original passwords that contain a combination or letters, numbers and even special characters (#, &, %) if allowed.
- Install and use anti-virus, anti-malware, anti-spyware and firewall software. Ensure that they are kept up to date by doing regular updates.
- Apply all security related operating systems and browser related updates as soon as they are available.
- Do not open any internet e-mails from unknown senders. Delete them immediately.
- Do not access financial websites from public or insecure computers.
- Do not access any suspicious web sites or download and install “free” software.
- Sign off from our services when you’re done instead of just closing or shutting your browser. Activate your “time out” tool to block access if you leave your computer.
- Learn about your rights and obligations regarding our relationship by reading our contract.
- Shred all canceled checks and financial records when no longer needed.

Things You Can Do to Protect Your Business

What to do…

- Thoroughly review payment orders and other instructions to us for accuracy and format before issuing them.
- Insist on a prompt review of account activity, canceled orders, confirmations and other communications we send you by someone other than the person initiating your transactions or usually accessing your account(s).
- Maintain deposit slips and other financial records in secure places.
- Give identity authentication and account information only to persons that are authorized to have and use it.

What no to do…

- Do not use information easily associated with you in your password, PIN or other access code
  (e.g. Date of birth, Social Security Number, Taxpayer Identification Number. Employer Identification Number name, etc.).
- Do not use names of people, sports teams, cities or common dictionary terms in a password, PIN or other access code to anyone.
- Do not put your password, PIN or other access code where others can get it.
- Do not use a password-saving automatic login tool.
- Do not share your password, security tokens for our services with any third party. We do not keep records of your passwords or login access nor will we ever ask you for it.
- Do not share your login access codes for our services with any third party.
- Do not delay telling us about any unusual or unfamiliar communications, requests or transactions that might involve our relationship.

Using a Computer

What to Look for

Fraudulent Email and websites; a criminal may send email that appears to come from us. It may ask you to access a website that looks like ours and supply information about you or your accounts. The email or website may also state your account will be disabled in some way if you don't supply your account information. This fraud is commonly called "phishing" or "spoofing". The goal is to get information from you in order to steal from you or others by appearing to be you. If you get such email that seems suspicious, just delete it. Let us know about it by contacting your Relationship Manager.

What to do…

- Scan computers regularly with software that protects your computer against viruses or spyware and provides firewall protection.
- Collect and install new security updates when your operating system requires to do so.
- Avoid unauthorized access to paper records.
- Promptly review your bank statements and other communications for accuracy.
- Completely erase information stored on a computer before disposing of that computer.

Remember this can be performed by professionals to ensure that all your data (if any) on your hard-desk completely erased.

- Read privacy policies for answers to questions about access and information security and how your information will be used. Set up your wireless communication equipment with encryption (password protection)
- Set up your wireless communication equipment with encryption (password protection)

What not to do…

- Don't share passwords, PINs or other credentials with anyone, including BTMU (H).
- Don't leave a computer unattended.
- Don't respond to emails requesting personal, financial, or identity information (like a User ID, Password, PIN, SSN etc.).
- Delete spam or suspicious emails from your Inbox. Don't click on links or open attachments from suspicious emails.
- Don't download files from unknown or untrusted websites.
- Don't access your MUFG Bank (Europe) services/information from insecure locations like internet cafes. Don't store sensitive information on your computer, including laptop and portable electronic devices.

Using a Telephone

We offer our customers a number of services that involve using the telephone (voice) to inquire or instruct us regarding their accounts. We use a number of methods to protect our customers. These methods may involve the following;

- Comparing signatures appearing on application/or email attachments with those of our files.
- Calling an authorized account holder to confirm that instructions are genuine.