集友銀行
Chiyu Banking Corporation Ltd.

April 2023

Important Notes on Precautions of Bogus Voice Message Phone Calls, Fake E-mails, Fake SMS and Fraudulent Websites

Chiyu Banking Corporation Ltd. ("Chiyu Bank") would like to remind its customers to stay vigilant to voice message phone calls purportedly from Chiyu Bank, fake e-mails, fake SMS and fraudulent websites, etc. Customers are advised to protect their personal information at all times.

In this regard, Chiyu Bank wishes to alert its customers to the following important notes:

1. Aware of the "Phishing" fraudsters send out emails or SMS purportedly from our bank, and request you to click on the embedded hyperlinks in the emails or SMS messages and enter your account details, passwords, personal information or credit card numbers etc.

2. Avoid logging into Internet /Mobile Banking or providing any sensitive personal information through hyperlinks or QR Code embedded in any third-party website, mobile Apps, emails or SMS.

3. Chiyu Bank will not notify customers of any irregularities or suspension of their bank or credit card accounts, and request customers to input their personal information or contact bank staff for identity verification through any pre-recorded voice messages or e-mails. Customers are also reminded not to rely solely on the incoming call display, e-mail address, SMS, website address or message content to identify the caller/sender.

4. Customers who are suspicious about the identities of the callers should request for the callers' contact numbers and names, etc. for verification and should not disclose their personal information during the process.

5. If customers would like to verify any phone calls, e-mails, SMS or website addresses purporting to be from Chiyu Bank, they should call Chiyu Bank's Customer Service Hotline at (852) 2232 3625 (press "8" after selecting language) or visit any of our branches for enquiry. Customers who may have disclosed their personal information to any suspicious person, should immediately contact Chiyu Bank or directly contact

the Hong Kong Police Force.

6. To access the Internet or Mobile Banking Service, customers should type the website of Chiyu Bank (www.chiyubank.com) directly into the browser address bar. They should not log into the Internet Banking or Mobile Banking through any hyperlinks embedded in e-mails from unknown sources.

7. If customers do not wish Chiyu Bank to use their personal data or provide it to any third party for the purpose of direct marketing, they may exercise their opt-out right by calling our Customer Service Hotline or visiting any of our branches.

"Protect your Personal Digital Keys, Beware of Fraudulent Links!" Please remember to stay alert and watch out for phishing SMS, emails and fraudulent websites. We will never request you to click on any hyperlinks embedded in SMS or emails for logging into Internet /Mobile Banking or request for your sensitive personal information e.g. login details or one-time password. If you are suspicious, please call our Customer Service Hotline at (852) 2232 3625 immediately.

Customers should be aware of the relevant security measures specified from time to time by us for the protection of customers. For the security information of Internet Banking, please browse www.chiyubank.com/chiyu/en_supp4_1.htm.

Meanwhile, please visit the HKMA website: (1) Beware of Phishing SMS and Emails and Education Videos (2) Protect your Personal Digital Keys and Education Videos, or refer to the Anti-Deception Resources on HKAB website.

A copy of the "Alert on Bogus Voice Message Phone Calls, Fake E-mails, Fake SMS and Fraudulent Websites" is attached for your reference.

Chiyu Banking Corporation Ltd.

集友銀行
Chiyu Banking Corporation Ltd.

Alert on Bogus Voice Message Phone Calls, Fake E-mails, Fake SMS and Fraudulent Websites

Scenario 1: Preventive measures against fraud

Do

- ✓ Request for the callers' contact numbers and names, etc for verification in case of suspicious calls.
- ✓ Call Chiyu Bank's Customer Service Hotline or visit any of our branches for verifying the authenticity of phone calls, e-mails, SMS or website addresses.
- ✓ Type the website of Chiyu Bank directly into the address bar of the browser for access to the Internet Banking Service.
- ✓ Stay vigilant to anything abnormal (e.g. request for inputting your credit card number, expiry date or verification code on the back of credit card, one-time password or personal data) during login to Chiyu Bank's website/Internet Banking.
- ✓ Review your services' limits regularly and to make necessary adjustment that suits your transaction needs.

Don't

- ✘ Disclose sensitive personal information (in particular the login and one-time passwords) to third party.
- ✘ Rely solely on the incoming call display, e-mail address, website address or message content to identify the caller/sender.
- ✘ Log into the Internet Banking and Mobile Banking or providing any sensitive personal information through any hyperlinks or QR Code embedded in any third-party websites, mobile Apps, e-mails or SMS from unknown sources.

Scenario 2: Follow-up action in case of disclosure of personal information to any suspicious person

Do

- ✓ Contact our staff by calling Chiyu Bank's Customer Service Hotline or visiting any of our branches immediately.
- ✓ Stay calm and contact the Hong Kong Police Force as soon as possible.

Don't

- ✘ Attempt to handle the case on your own and delay contact with our bank staff or report to the Hong Kong Police Force.