Protection from Fraud and Identity Theft

01 March 2016

Dear Valued Customer,

----------**SECURITY ALERT NOTICE** ----------

Please note, that hoax emails purporting to originate from BRED Bank (Fiji) Pte Ltd are in circulation. The contents and resultant links appear genuine but these are **fraudulent** and have not been sent by **BRED Bank (Fiji) Pte Ltd**.

As stated in our Direct Banking Service Terms and Conditions BRED Bank (Fiji) Pte Ltd **will never** send you e-mails asking for confidential details of your account/ PIN / Password or personal parameters such as date of birth, mother's maiden name etc.

Beware of anyone asking you for such information on behalf of the bank through e-mails or phone calls.

Please **do not** provide your bank account details to emails claiming to deactivate your account, offering a job or claiming that you have won a lottery.

When you receive such emails, **please immediately delete** without further action, and refer to our e-channels department for further assistance.

While it is our relentless endeavour to provide you with the best of online services and facilities, the Bank is not responsible for any erroneous or wrong transactions made by you. The Bank shall also not be responsible for misuse of your account arising from any wrong, inadvertent or other kind of disclosure of such details by you.

Please refer to our Safe Banking section on our website https://www.bred.com.fj for guidance.

---------- **END OF NOTICE** ----------

For further information you may:

Email: e-channels@bred.com.fj
Telephone: (679) 323 0218

Kind Regards,
Customer Service.

Table of Contents

Protection from Fraud & Identity Theft 2
Simple Steps to Secure Your Devices 2
Setting Up Your Computer and/or Mobile Device 3
Adding Security Software 3
Internet Safety Tips 3
Guidelines for Safely Banking Online 3
Guidelines for Strong Passwords 4
Guidelines for Safe Web Browsing 4
Guidelines for Safe Email 5
Guidelines for Safe Instant Messaging 5
ATM & Mail Safety Tips 5
Precautions When Using ATMs 5
Guidelines for Protecting Your Mail 6
Know the signs of fraud 6
Email Fraud 6
Website Fraud 6
Phone Fraud 7
Mail Fraud 7
Credit/Debit Card Fraud 7

Protection from Fraud & Identity Theft

The best way to defend yourself against financial fraud is to know how criminals operate. The more you know, the less likely you are to become a victim.

Here are some simple steps you can take today to surf, shop and bank online safely.

Simple Steps to Secure Your Devices

Chances are your computer contains a goldmine of personal information. Make sure you're taking the necessary precautions to protect it.

Most people think their computers are secure. But a study by security authorities shows they're actually at risk because of out-dated security software, infrequent virus scanning or not activating their firewall. To see if your computer security is updated and active, review the tips below.

Setting Up Your Computer and/or Mobile Device

- Use a newer operating system such as Windows 7 or Mac OSX. They're more secure.
- Download security patches and updates. Turn on automatic updates so you've got the latest fixes to problems as they arise.
- Disable "File and Printer Sharing" on your computer to prevent unauthorized access.
- Increase the security settings for your operating system.
- Use a current web browser and keep it updated. BRED Bank (Fiji) Pte Ltd's Internet Banking Solution (Direct Banking) is accessible with the following browsers:
  - Microsoft Internet Explorer™
  - Google Chrome™
  - Mozilla Firefox™
  - Apple Safari™ (PC only)
- Set your browser to block pop-ups.
- Turn your computer off when you're not using it. If you're not connected to the Internet, you can't be hacked or infected.

Adding Security Software

- Use new anti-virus software to protect against viruses and spam.
- Use an anti-spyware program.
- If your operating system has a built-in firewall, enable it. Or install a third-party firewall to block hackers.
- Use a secure Password to prevent access when you're away from your computer.
- Use encryption software to protect data stored on your laptop, PDA, cell phone or other wireless device.

Internet Safety Tips

Cyber criminals are using more sophisticated methods to steal your information. Follow our tips to stay two steps ahead.

If you've followed our guidelines for securing your computer & mobile device, you've already made it harder for someone to steal your identity. But all the safeguards in the world won't help you if you give your personal information away. So be smart and follow the guidelines below to protect yourself online.

Guidelines for Safely Banking Online

- Access online banking sites by typing the URL directly into the address bar.. Be aware of pop-ups as they may indicate you have malware on your computer.
- Report pop-ups to your financial institution.
- Do not click on links in an email l unless from a trusted source. Access the bank using a bookmark or address you know is safe.
- Check for anything unusual, unprofessional or out of place such as a slightly altered domain name like www.bred.com, www.bbf.com or www.bred-security; an imperfect logo; or urgent account verification requests.

- Review the website's privacy policy to learn how your information will be used and protected.
- Don't use the same Password for banking that you use for other online accounts.
- Don't use public computers to do your banking, including those at libraries, Internet cafes and schools.

Guidelines for Strong Passwords

- Don't share your Password with anyone.
- Memorize your Password. Don't write it down or store it on your computer.
- Use upper and lower case letters, numbers and symbols.
- Avoid common words or obvious names. Think of a phrase that's memorable to you but not to others. (For example, "My favourite pet has one white eye and floppy ears" becomes "MfPh1weAfE".)
- Use Passwords that are at least eight characters long.
- Change Passwords regularly (at least every 90 days).

Guidelines for Safe Web Browsing

- Don't respond to unsolicited requests for account information.
- Don't click on pop-ups. Better yet, set your browser to block them.
- Don't give out personal information to blogs, forums and other social networking sites.
- Don't visit unsafe sites. You could open yourself up to a flood of spam, pop-ups and spyware.
- When shopping online, use secure sites that encrypt your credit card information.
- Be suspicious of odd error messages. Don't click on them or respond to them. Scan your computer to remove any virus or spyware.
- Scan your computer files regularly, once a week at a minimum.

Guidelines for Safe Email

- Don't open email from someone you don't know. Read subject lines carefully. Don't be tricked by a friendly tone or urgent request.
- Turn off the preview pane in your email program.
- Don't click on links or attachments in unsolicited email, especially if they say a problem is urgent or includes an attached file that ends in ".exe."
- Don't give out personal information. Check a website's privacy policy before you give them your email address.
- Delete email from unknown sources immediately. Use your junk mail filter.

NOTE: If BRED Bank (Fiji) Pte Ltd sends email to your personal email address, it will always include a personal or account identifier. Any links included will be to a BRED Bank (Fiji) Pte Ltd web site information page, not directly to a page that requires log-in credentials or personal information.

Remember: No one at BRED Bank (Fiji) Pte Ltd will ever ask you for your Password.

Guidelines for Safe Instant Messaging

- Block people you don't want to know, especially complete strangers. Adjust your IM settings so that only people on your buddy or friends list can IM you.
- Don't reply to strangers, especially if their messages are rude or annoying. It could be a predator.
- Don't click on unsolicited links or attachments. They could contain a virus or spyware.
- Don't create a profile that includes personal information. It can open you up to harassment and attract predators.
- Know your children's online friends and supervise their chat areas.
- Restrict your Privacy settings on any social networking site.

ATM & Mail Safety Tips

To open new accounts in your name, thieves don't have to look any further than your mailbox. Pre-approved credit offers and outgoing bills may be all anyone needs to steal your identity. More sophisticated methods involve skimming or copying your card at an ATM. To reduce your risk of fraud, put our safety tips into action.

Precautions When Using ATMs

- Memorize your PIN. Don't write it down or keep it in your wallet or purse.
- Protect your PIN. Cover the keypad while you enter the number.
- Use ATMs under video surveillance or those located inside a bank lobby.
- Conduct ATM transactions during the day. Most ATM crime happens at night.
- Watch out for shoulder surfers with binoculars or cameras.
- Don't accept offers of "help." Leave immediately.
- Be suspicious of signs telling you to use a specific machine. The ATM may be fitted with a skimming device.
- Report anything suspicious or strange to your bank or financial institution.

Guidelines for Protecting Your Mail

- Collect incoming mail promptly. Don't leave it in your mailbox overnight or on weekends.
- Consider using a locking mailbox or rent one at the post office.
- Don't use the red flag to draw attention to your outgoing mail.
- Deposit outgoing mail in official postal service collection boxes.
- Shred unwanted documents containing personal information such as credit applications, convenience checks, bank statements and bills.
- Check your monthly financial statements and bills for accuracy.
- If you don't get monthly financial statements and bills when expected, contact the sender.

Know the signs of fraud

When logging on, a pop-up window appears stating the service is not available and to try later. A misspelled domain name in the address line. Lotteries that charge a fee to collect your winnings. Requests to pick up or send cash to a person overseas and they offer to share the money. All of these tricks and more have been used to take someone's money or identity. To avoid being conned, learn the tell-tale signs below.

Email Fraud

Beware of Phishing

So-called "phishing" emails appear to be from legitimate companies. Typically, they warn you of an urgent problem with your account and trick you into clicking on a link that takes you to a phony website. Remember, no reputable company would request personal information via email. Other warning signs that an email is fraudulent:

- Generic salutation such as "Dear user" and/or impersonalized information in the text of the email.
- The logo may be distorted or stretched.
- The link in the email doesn't match the URL of the legitimate site.
- There's an attachment or link that may launch a virus or spyware on your computer.

Website Fraud

Phishing Websites

Fraudulent (phishing) emails may direct you to a bogus or spoof site that's often very convincing. Look closely for these tell-tale signs:

- The site threatens to shut down your account unless you verify your personal information.
- The site returns an error message and asks you to log in.

- The URL isn't quite right. For example, you see www.bred.com or www.brd.com instead of www.bred.com.fj. The URL may also contain numbers (such as an IP address) or an "@" symbol.
- The padlock icon is out of place. It should be in the browser status bar in the lower right and not within the web page.
- When you double-click on the lock icon, you get a warning that the site address doesn't match the security certificate.
- The logo may be distorted or stretched which indicates it's been copied.
- Spelling and grammar mistakes.
- If there's a phone number on the fake website, it doesn't match the phone number on your account statement.
- You can't link to a home page from the fraudulent site.

Phone Fraud

Recognizing Phone and Text Fraud

Never give out personal information over the phone unless you initiate the contact. Be suspicious of the following:

- Automated messages with urgent requests to verify your account.
- Voicemails asking you to call a number with an "809", "284", "876" or other international code. You'll end up with an expensive phone bill.
- To claim a lottery prize or other winnings, you're asked to dial a two-digit code preceded or followed by the "#" or "*" key (for example, *79 or 72#) and then an 800 number. This is a call-forwarding scam.
- Text message asking for urgent confirmation of personal or account information.

Remember: No one at BRED Bank (Fiji) Pte Ltd will ever ask you for your Password.

Mail Fraud

Spotting Mail Fraud

If it sounds too good to be true, it's probably a scam. Be suspicious of the following:

- Pre-approved credit offers that charge a fee to get your card.
- Job scams asking you to pay for more information.
- Work-at-home schemes that require you to buy something before you can start work.
- Any request to call a 900 number (All you'll get is a large phone bill.)
- Donation requests to unregistered charities.
- Sweepstakes and lotteries where you have to pay to receive your prize or those involving a foreign country.

Credit/Debit Card Fraud

Watch Out for Skimming

Card fraud can occur anywhere you make a transaction including restaurants, gas stations and other retail locations. Beware of the following:

- Swiping your card twice, once for your purchase and a second time through a skimming device (As a general rule, don't let your card out of your sight.)
- Someone looking over your shoulder at the register, EFTPOS terminal or ATM.
- Receipts and copies. Ensure that you collect all your receipts. File them away safely for future reference or destroy as appropriate.

END OF DOCUMENT