AUSTRALIA

CUSTOMER EDUCATIONAL AND GUIDANCE MATERIALS FOR SCAM CALLS AND SCAM SMS

TYPES OF SCAM CALLS AND SMS RELATED FRAUD RISKS

There are many types of scam calls and SMS which are designed to obtain a benefit from you, or cause a loss, by deception, dishonesty, or other means. Some examples of common red flags to be aware of when trying to spot a scam call and/or SMS are:

- Receiving an offer that seems too good to be true or a notice that you are the recipient of money, prize, or other benefit you did not expect to receive;
- Someone asks for access to your computer, phone or other device to help fix it or get rid of malware or spyware;
- Receiving a threat to pay money you do not owe;
- Receiving an alert that appears to be from your bank or another institution you trust about a problem with your account, asking you to confirm personal information, or provide money;
- Someone you do not know reaches out to you with personal information you did not provide them with;
- Receiving calls or SMS from a number you do not know multiple times - even if it is a local number - scammers can disguise their number to make it look like they are calling you from somewhere local;
- Receiving a robocall or recorded message asking for payment or personal information; or
- Receiving a call or SMS that creates the sense that something is an emergency and that there will be negative consequences for you if you do not provide them with your personal information, payment, or click a certain link.

To assist in awareness and identification of scam calls and SMS, the Australian Competition and Consumer Commission (ACCC) compiled a list of the most common types of scams that you may encounter in the The Little Black Book of Scams.

INFORMATION ABOUT HOW TO BLOCK UNWANTED SCAM CALLS AND SMS

Most mobile phones allow you to block a telephone number so you would no longer receive any suspicious or unwanted scam calls and SMS. Please consult the information provided by your phone manufacturer or mobile network provider for information on how to block a telephone number from your specific mobile device.

HOW TO MITIGATE THE RISKS ASSOCIATED WITH SCAM CALLS AND SMS

While this list is not exhaustive, there are some steps you can take to try to mitigate the risks posed by scall calls and SMS:

- Protecting your personal information and not share it with unknown or unsolicited callers;

- Contact your financial institution immediately if you believe you have lost money to a scammer;
- Lock your devices with secure PINs;
- Select strong PINs and passwords (e.g. Not “1234” or “0000” or “password” etc.);
- Change PINs and passwords regularly;
- Change your default PINs and passwords on newly acquired devices;
- Ensure your voicemail PINs are secure;
- Disable PABX ports and features that are not used (e.g. remote call-forwarding);
- Do not respond to missed calls or SMS from unknown international numbers, unknown Australian numbers or an unknown source;
- Do not click on URLs or making return calls to telephone numbers contained in the SMS from unknown international numbers or unknown Australian numbers or an unknown source;
- Block suspicious or unknown Australian numbers or international numbers on devices and use of blocking services or products, where available, on landlines; and
- Allow unknown calls to go to voicemail and then listen to any message left to ascertain if this might be a genuine call.

REPORTING SCAM CALLS & SMS

If you believe you have received scam calls and/or SMS you can also report it to Scamwatch. Scamwatch also provides resources to help you mitigate any damage and protect yourself from future loss, which are available here.

ADDITIONAL INFORMATION

For more information on scams and where you can seek assistance if you are the victim of a scam please consult the following resources:

- Scamwatch
- Stay Smart Online
- Little Black Book of Scams