SOUTH SILVER SDN BHD

SOUTH SILVER SDN. BHD.
Registration No. 200101012945 [548702-W]

TERMS AND CONDITIONS

PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING MMM CREDIT SERVICES.

MMM CREDIT Services is owned by South Silver Sdn Bhd ("**South Silver**"). By using this MMM CREDIT Services you are deemed to have read and accepted these TERMS AND CONDITIONS. Please refrain from using this MMM CREDIT Services if you do not agree to all or any of these terms and conditions. South Silver shall not be liable for payment of any costs or expenses incurred as a result of downloading and using this MMM CREDIT Services, including any operator network and roaming charges.

1. Content
(a) The contents of our MMM CREDIT Services are intended for your personal non-commercial use only. Graphics and images on this MMM CREDIT Services are protected by copyright and may not be reproduced, translated, or appropriated in any manner without our written permission. Modification of any of the materials or use of the materials for any other purpose will be a violation of South Silver's copyright and other intellectual property rights and the copyright and intellectual property rights of the respective owners.
(b) If you download any software from the MMM CREDIT Services, the software, including any files, images incorporated in or generated by the software, and data accompanying the software (collectively, the "Software") are licensed to you by South Silver. South Silver does not transfer title to the Software to you. You own the medium on which the Software is recorded, but South Silver retains full and complete title to the Software, and all intellectual property rights therein. You may not redistribute, sell, decompile, reverse-engineer, disassemble or otherwise deal with the Software nor extract the source code of the MMM CREDIT Services.

2. Use of MMM CREDIT Services
(a) You agree to use this MMM CREDIT Services in accordance with these terms and conditions and for lawful and proper purposes. You agree to be responsible for all matters arising from your use of this MMM CREDIT Services. Further, you agree not to use this MMM CREDIT Services in any manner which breaches any applicable law or regulations or causes or which may cause an infringement of any third party rights, not to post, transmit or disseminate any information on or via this MMM CREDIT Services which may be harmful, obscene, defamatory or illegal or create liability on South Silver's part, not to interfere or attempt to interfere with the operation or functionality of this MMM CREDIT Services and not to obtain or attempt to obtain unauthorized access, via whatever means, to any of South Silver's systems. (b) If South Silver (in its sole discretion) believes that you are in breach, or will be in breach, of any of these terms and conditions, South Silver reserves its right to deny

you access to this MMM CREDIT Services without giving you a reason and/or without further reference to you.

3. Other Sites
Our MMM CREDIT Services provides links to other sites and vice versa merely for your convenience and information. We shall neither be responsible for the content and availability of such other applications that may be operated and controlled by third parties and by our various branch offices worldwide, nor for the information, products or services contained on or accessible through those MMM CREDIT Services. Your access and use of such MMM CREDIT Services remain solely at your own risk. South Silver will not be liable for any direct, indirect, consequential losses and/or damages of whatsoever kind arising out of your access to such applications.

4. No Warranties
We provide no warranty, whether expressly or implied, of any kind including but not limited to any implied warranties or implied terms of satisfactory quality, fitness for a particular purpose or noninfringement. All such implied terms and warranties are hereby excluded.

5. Disclaimer
South Silver does not warrant that the functions contained in the materials will be uninterrupted or error free, that defects will be corrected or that this MMM CREDIT Services or this server that makes it available is free of any virus or other harmful elements. South Silver does not warrant or make any representations regarding the correctness, accuracy, reliability or otherwise of the materials in this MMM CREDIT Services or the results of their use.

6. Liability
(a) By using our MMM CREDIT Services you agree that we will not be liable under any circumstances, including negligence, for any direct, indirect or consequential loss arising from your use of the information and material contained in our MMM CREDIT Services or from your access to any of the linked sites. We are also not liable nor responsible for any material provided by third parties with their own respective copyright and shall not under any circumstances, be liable for any loss, damages or injury arising from these materials.
(b) Any South Silver publication may include technical inaccuracies or typographical errors. Changes may be made to these publications from time to time and incorporated in new editions of these publications. At any time without notice, these publications are subject to improvements and changes in service by South Silver.
(c) The information contained in this MMM CREDIT Services is for informational purposes only and is provided to you on an “as-is” basis. We do not guarantee the accuracy, timeliness, reliability, authenticity of completeness of any of the information contained on this MMM CREDIT Services. We are not liable for any information or services which may appear on any linked MMM CREDIT Services.

7. Changes and Modifications
(a) We reserve the right at our absolute discretion and without liability to change, modify, alter, adapt, add or remove any of the terms and conditions contained herein and/or change, suspend or discontinue any aspect of this MMM CREDIT Services.
(b) We are not required to give you any advanced notice prior to incorporation of any of the above changes and/or modifications into this MMM CREDIT Services.

8. Suggestions, Comments and Feedback
Any communication you send to our MMM CREDIT Services or otherwise to us by electronic mail shall be treated as non-confidential. Your comments, suggestions, questions, feedback and the like regarding the content and/or our services in general, including any ideas,

inventions, concepts, techniques or know-how disclosed therein may be used by us for any purpose, including the development, manufacturing and/or marketing of goods and/or services, and in such circumstances, you are not entitled to any reward or compensation of whatever nature from us. FOR THIS PURPOSE, WE RESERVE THE RIGHT whenever necessary to disclose your personal information without your consent to our affiliates, authorised agents, government/security agencies or the providers of similar services, in whatever country they may be located as set forth in our Privacy Policy.

9. Exclusions
The exclusions and limitations described herein shall apply only to the extent permitted by law, without prejudice to our rights to seek legal redress in accordance with the applicable laws.

10. Applicable Law and Jurisdiction
These TERMS AND CONDITIONS and this MMM CREDIT Services's content shall be governed and construed in accordance with Malaysian laws, and the courts of Malaysia shall have exclusive jurisdiction to adjudicate any dispute which may arise in relation thereto.

11. Data Protection
Please also see South Silver's Privacy Policy regarding information you provide to South Silver when you register for, download and/or use this MMM CREDIT Services.

12. Conflict Between English Text and Other Translation
If there is any conflict or discrepancy between the English text of these TERMS AND CONDITIONS and any translation thereof, the English text shall prevail and supersede any other translation or any other version in any other language.

SECURITY ALERT

INTRODUCTION

South Silver Malaysia Sdn Bhd ("**South Silver**", "**we**" or "**us**") is committed to ensuring that all activities and/or transactions performed online is secure, safe and confidential. We have made it a point to reinforce our systems with safeguards to preserve a secure environment for you to carry out your transactions and now wish to provide you with safety precautions that are practical, effective and in certain instances obligatory for online lending.

We treat the security of your account with utmost priority and to this end, we use a variety of security measures to make sure that your account is secure. However, it is your responsibility to ensure that your account is kept safe from unauthorized access and attempts to use it for fraudulent purposes at all times. You must ensure that you do not share access of your account with any person other than yourself and keep your login details safe. It is your responsibility to keep your account secure and be responsible for transactions carried out using your account. You should never conduct any transactions on behalf of any third parties or allow any other individual to conduct a transaction on your behalf. You should never use the South Silver App or submit any transactions on a 'jailbroken', 'rooted' or otherwise modified device. In addition, you must only download or use the South Silver App on mobile devices installed with the latest and most secured operating system(s) available for the mobile device. If you find or suspect any unauthorized use of your account or any other security breach, you must notify us immediately using any of the contact methods provided so that we can take all the necessary steps to prevent further unauthorized use.

We also regularly monitor the apps distribution platforms and will report fake app to the app distribution platforms for their further action to prevent such fake app from being made available for download by users. We also monitor sources identifying fake/phishing websites and will take the necessary action to report the same to the appropriate parties (overseeing or hosting these sites) for the same to be taken down in order to safeguard users from falling prey to scams or fraud sites guising as South Silver's official website.

In any event, you can always validate the authenticity of South Silver's app through Apple's App Store and Google's Play Store, as the app is signed by the South Silver developer account. Notwithstanding, you must only download the South Silver app **from either Apple's App Store or Google's Play Store**. You must **not** download the South Silver app from any other app sites, websites or app forums as they will most probably be fake or phishing sites which we do not authorize or approve to publish the South Silver app.

PROTECT YOURSELF

In addition to our security measures you also play an important role in safeguarding your transactions made through your computer and mobile devices. We recommend that you do the things as listed below:-

1. Install anti-virus and anti-malware

Protect your devices from virus and malware by installing anti-virus and anti-malware software. To maximise your protection, update them regularly to make sure you always have the latest virus definition.

2. Avoid rooting or jailbreaking your mobile devices

It is not advisable to use a rooted or jailbroken device as they are more vulnerable to fraudulent attacks. A rooted or jailbroken device has minimal security, making it easier for a fraudster to gain access to your personal details and other information stored or transmitted through your device.

3. Install a personal firewall
Firewall software and/or hardware helps provide a protective shield between your computer/mobile devices and the Internet. This barrier can help prevent unauthorised people gaining access to your computer/mobile devices, reading information from it or placing viruses on it while you are connected to the Internet.

4. Install anti-spyware software
Spyware is a general term for hidden programs on your computer/mobile devices that track what you are doing on your computer/mobile devices. Spyware is often bundled together with file sharing, email virus checking or browser accelerator programs, and is installed on your computer/mobile devices without your knowledge to intercept information about you and your computer/mobile devices. The type of information gathered can include personal Internet usage, and in some instances, confidential data such as passwords. You can download and run a specialist program designed to help identify and remove threats from spyware. Like an anti-virus program, it also needs to be regularly updated in order to recognise the latest threats.

5. Keep your browser and operating system up-to-date
From time to time security weaknesses or bugs are found in browsers and operating systems. Usually 'Service Packs' are issued by the software company to make sure these are fixed as quickly as possible. You should make regular checks on your software vendor's website and apply any new security patches as soon as possible to ensure you have the most updated security features available.

6. Avoid running programs or opening email attachments from any source you do not know or trust
You should not install software or download any files from websites (e.g. programmes, games, and screensavers) that you aren't completely sure about. We also recommend that you scan all email attachments for viruses and avoid opening any from people or organisations that you do not know or trust. However, some viruses may forward infected emails to everyone in an address book, therefore you can also get an infected attachment from someone you know. If you are not sure what is in the attachment, do not open it.

7. Be cautious when using public or shared computers/networks
If you access your accounts using a computer in a cyber café, a library or your workplace, try to ensure the computer has the latest antivirus, firewall, antispyware and browser software installed. Although Wi-Fi is a convenient way for you to access the Internet, it is not advisable and we caution you against accessing your account via public Wi-Fi connection especially in public places like airports, hotels or shopping malls.

8. Be proactive
You should regularly be kept informed of your accounts by checking all transaction alerts in a timely manner and to check account balances on a regular basis to detect any unauthorised transaction, error or discrepancy and to report the same to South Silver in the event any unauthorised transaction, error or discrepancy is detected.

TYPES OF THREAT

Protect yourself from becoming a victim of online fraud. Listed here are the four major types of threat: -

1. Computer Viruses

Computer viruses are malicious software which are also known as malware that infect computer devices and perform harmful activities. It can be viruses, Trojans and spyware to “PC Optimization” programs that harm your devices, interfering with the system's operations, corrupting data, logging user's keystrokes and stealing private information.

2. Phishing Scam

“Phishing” is a type of identity theft where criminals blast emails to mass audience purportedly from South Silver in their malicious attempt to bait user into fake websites. It usually comes with a link that the user can click on which will direct the unsuspecting victim to a fake website and the user will be asked to disclose confidential or financial information, passwords, and credit card numbers along with highly confidential information. More often than not, the emails may imply a sense of urgency or serious consequences should the user did not respond to it. For example, it could be worded in such a manner that if no action is taken, the account will be suspended.

3. Phone Scam

This comes in the form of the phony disguises as a South Silver staff or someone you can trust who calls you. The victim is usually informed of some irregularities with the account in question and action needed to be taken immediately. Usually the user will be “alerted” of “missing money” or that the user's account has been compromised by possible scams by the phony. To rectify user’s losses or to prevent the “scams”, the phony will instruct the user to perform an online transaction to a third-party account.

4. SMS Scam

These are fraudulent SMS sent to user victims informing them that they have won a cash prize or requiring them to call a given number to confirm on a transaction involving the user's credit card or account information. To claim the prize, the victim is told to transfer a certain amount of money to a third party accoun. The victim is tricked into divulging the registered User ID and Password to the fraudster. Having done as instructed, the victim has unknowingly given the fraudster access to their account.

What should you do?

- Do not click on adware or suspicious URL sent through SMS/Messaging app.
- Do not use public Wi-Fi networks that are suspicious for online transactions.
- Do not save your login details on a public computer.
- Do not respond to suspicious emails or SMS content from suspicious links or unsolicited senders seeking personal or confidential information.
- Do not respond to a request seeking for you to validate or verify your personal and confidential information.
- Do not respond to any SMS or call from an unknown person asking details of any transaction.
- Do not respond to any call from a person claiming to be from Bank Negara Malaysia. Their officers will never call to ask you about an online transaction.
- Clear your cache (information stored in your computer or app memory) each time you log out.
- Change your password frequently. If you think your password has been compromised, contact us to reset your password.

- Avoid downloading free programs. These may incorporate hacker-friendly software.
- Install anti-virus or anti-malware software.
- Refrain from rooting or jailbreaking your mobile devices as this could compromise its security features.

Take note that on principle, we would NEVER ask you to validate personal or confidential information via e-mail. If for some reason you have entered sensitive information after clicking on a link or if you suspect that you've been a victim of fraud, please contact us immediately.

5. Managing PASSWORD & Personal Details

- DO memorize your login password.
- Ensure no one is observing when you key in your login password.
- DO NOT create PASSWORD that is sequential, repetitive and obvious (such as date of birth, identity card number, etc.)
- DO NOT write your PASSWORD on your card, anywhere near it or unsecured places.
- NEVER disclose your PASSWORD (or username, password, security questions/answers, etc) to others.
- CHANGE your PASSWORD periodically for precaution.

6. Managing Statements & Related Documents

- CHECK your loan statement promptly and report immediately on any transactions or lending that you do not recognize or did not apply.
- KEEP South Silver updated with your latest contact number and/or email address to allow South Silver to perform verification of unusual or suspicious activities or lending. Notify South Silver on your change of mailing address too.

7. Scams

- NEVER respond to email, website or phone inquiry is that request you to provide your card details or ask you to go to a website to verify card or personal details. These are called "Phishing" scams.
- DO NOT provide your card details over the phone unless you have validated the company or individual you are speaking with.

8. Compromise of account

Where you have notified us, or we reasonably believe that your account has been compromised, we may stop, block or suspend your access to and use of your account and/or any services provided by us. We also have the right to disable or change any user name or password (if possible), whether chosen by you or provided by us to ensure the security of the account, in our sole discretion. Note that any act or omission of South Silver in relation to any steps to be taken as set out above does not make South Silver liable to you for any loss or damage arising from the result of your failure to keep your account secure and notifying us of the same.

If you believe that a transaction was made without your authorization, you must contact us immediately. We will conduct an investigation and may provide refunds of unauthorized transactions unless:

- you have acted fraudulently;
- you have intentionally or negligently compromised the security of your account or failed to keep the details you use to access the account secure;

If our investigations result in any special circumstances deviating from the above and affect the outcome of your liability and/or eligibility for a refund, we will notify you. Note that we have no responsibility towards you for any loss caused by unauthorized access prior to you notifying us. A charge may also be applied for any refund request if the unauthorised use, loss, theft or misuse of the account was caused by your error, carelessness or negligence.

In cases where we have reason to believe that you have acted fraudulently, we may decide not to allow any refund to you, investigate the circumstances further or even forward the matter to law enforcement authorities. If an investigation (whether by us or the authorities) results in a finding of fraud by you, we may charge you for costs incurred by us in carrying out such investigation and further deduct these monies from your account.