集美證券網上證券服務及流動網絡證券服務

本公司十分重視網上交易安全，建議您詳閱本公司提供的各項保安措施：

一、 防範偽造網站電郵及流動應用程式

- 您應透過輸入本行網址、書籤或登入網上證券或流動網絡證券服務。切勿透過電郵、網上的超連結或附件登入或提供個人資料(包括密碼)。
- 您必須經常保持警覺，注意任何試圖冒充本行網址的偽造網站。本行的網址為 www.jimei-investment.com。
- 本行絕不會發出附有接駁至交易網站的超連結電郵，亦不會以電郵方式向客戶索取帳戶號碼、網上用戶帳號/自選登入名稱、密碼或任何個人資料。
- 您切勿透過任何電子郵件或網上搜尋器提供的超連結使用網上證券服務及 / 或流動網絡證券服務。
- 檢查登入網頁及過程有否異樣(如出現可疑的彈出視窗、被要求提供額外的個人資料、及/或電腦操作出現異常緩慢的情況)。如您發現可疑電腦運作情況，建議您應立即登出網上證券服務，並利用防毒軟件(附有最新的病毒定義檔)為電腦進行病毒掃描。

二、 我們如何保障您安全地使用網上證券及流動網絡證券服務

- 我們採用 Secure Socket Layer(SSL)的加密技術，保障您的個人及交易資料在網上傳送途中的保密性。
- 我們的網頁伺服器設有防火牆，防止未經授權人士進入本行系統。
- 如您忘記登出網上證券服務及 / 或流動網絡證券服務，您的網上連線會在短暫的靜止狀態後，自動終止接駁，防止任何未經授權的交易。
- 當我們發現登入密碼連續 5 次輸入不正確後，您的網上證券服務及 / 或流動網絡證券服務會即時被暫停。

三、 您如何保護個人安全地使用網上證券服務及 / 或流動網絡證券服務

1. 使用證券服務時須注意的安全措施

網上證券服務

- 切勿在公眾地方使用公用電腦，如網上咖啡室或網吧，登入證券服務。

- 當使用 Wi-Fi 無線上網時，使用可信賴的 Wi-Fi 無線網絡或服務提供者，而非公共無線網絡，並啟用保安措施，例如盡可能使用 Wi-Fi Protected Access（WPA, 一種保護無線電腦網絡安全的系統）。
- 切勿透過任何電子郵件、電話短訊、應用程式、社交網絡、可疑的快顯視窗或網上搜尋器提供的超連結登入網上證券服務。
- 請緊記於登入網上證券服務前關閉其他瀏覽器視窗。
- 在登入網上證券服務前，必須確保您正連接至本行網上證券服務，其網址為 http://www.jimei-investment.com。
- 登入網上證券服務時，請確定身旁沒有其他人在窺視您的客戶編號、登入名稱和密碼資料。
- 請檢查上一次登入網上證券服務的日期和時間。如果您對所顯示的資料有任何懷疑，請立即與本公司聯絡。
- 如登入網上證券服務時遇上可疑情況(例: 電腦反應極為遲緩、登入步驟有異或被要求提供額外資料)，應立即停止登入並通知本行。
- 登入網上證券服務後，如需要閱覽其他網頁，請先登出網上證券服務。
- 切勿在未登出網上證券服務前離開電腦。
- 使用網上證券服務後，請緊記按「登出」離開，並關閉瀏覽器。
- 定期查閱證券戶口結餘及交易紀錄。如發現任何錯漏或未經授權的交易，請立即通知我們。

流動網絡證券服務

- 在登入流動網絡證券服務前，必須確保您正連接至本行流動網絡證券服務。
- 切勿安裝來源不明的軟件至您的流動裝置。
- 流動裝置須安裝和定期更新防毒軟件和防間諜軟件。
- 在公眾地方透過智能手機使用流動網絡證券服務時，應注意是否被人窺視您的流動網絡證券戶口登入資料。
- 切勿記錄流動網絡證券服務登入名稱及密碼在流動電話內。
- 避免與他人分享使用流動裝置，及使用您的流動裝置登入流動網絡證券服務。
- 設定難以猜破的鎖機密碼及自動上鎖功能，以防止他人未經許可使用您的流動裝置。
- 請使用最新版本的操作系統及瀏覽器。不應使用已被破解（「破解版」）的流動裝置，以免在登入流動網絡證券時出現保安漏洞。
- 請選用您的流動電話網絡供應商提供的網絡來使用流動網絡證券服務。避免透過公共無線網絡。
- 使用流動裝置原廠提供的瀏覽器，避免使用由其他來源下載的新安裝瀏覽器。
- 關閉無需使用的無線網絡功能(如 Wi-Fi、藍芽、NFC)。如需使用 Wi-Fi，應選用加密的網絡，並移除不必要的 Wi-Fi 連線設定。
- 定期清除手機瀏覽器內的暫存檔案及瀏覽記錄。
- 刪除過期及機密的流動短訊，以及定期刪除瀏覽器瀏覽記錄。
- 登入流動網絡證券服務時，請確定身旁沒有其他人在窺視您的登入名稱和密碼資料。
- 請檢查上一次登入流動網絡證券服務的日期和時間。如果您對所顯示的資料有任何懷疑，請立即與我們聯絡。
- 登入流動網絡證券服務後，如需要閱覽其他手機應用程式，請先登出流動網絡證券服務。
- 切勿在未登出流動網絡證券服務前離開流動裝置。

- 使用流動網絡證券服務後，請緊記按「登出」離開。
- 定期查閱證券戶口結餘及交易紀錄。如發現任何錯漏或未經授權的交易，請立即通知我們。
- 請及時查閱本行發出的電郵，並查核交易紀錄。若發現可疑情況，應立即通知本行。

2. 保管您的密碼、用戶帳號、自選登入名稱及個人資料

- 請於首次使用網上證券服務時立即更改您的私人密碼。
- 緊記要將您的密碼、客戶編號、登入名稱及個人資料保持機密及小心保全。
- 切勿向任何人（包括本行職員及警方）透露您的密碼，亦不應透過任何方法如電郵、電話或親自隨便向任何人透 露您的個人資料，如香港身分證號碼、電話號碼、出生日期。
- 切勿將您的網上證券登入資料與本行發放的一次性密碼貯於同一裝置。
- 選用一個安全的密碼。
- 為提高網上證券服務及 / 或流動網絡證券服務之安全程度，登入密碼格式須由 8-20 位數字及英文字母組合。
- 請設定難以猜破及與其他服務不同的密碼，並定期更新。切勿記錄密碼在電腦、手機或當眼位置。
- 定期或懷疑密碼外洩時更改您的密碼。
- 應為不同服務設定不同的密碼。
- 切勿容許任何人士使用您的網上證券服務及 / 或流動網絡證券服務戶口。
- 如您使用別人的電腦或流動裝置進行交易，必須於登出後清除瀏覽器內的暫存資料，以確保密碼沒有儲存於電腦或流動裝置內。
- 切勿將用作雙重認證的流動裝置交由其他人士保管、控制或亂放。
- 切勿在流動裝置下載或安裝來自流動短訊所接收的程式。
- 你應替所用電腦或流動裝置設定密碼，以防止未經授權人士於您離開電腦或流動裝置時擅自取用你的資料。
- 如果您更改了聯絡資料，請通知本公司。

3. 保護您的電腦或流動裝置

- 確定您所使用的電腦操作系統及應用軟件仍受供應商支援，並啟動自動更新功能，定期從可信賴的來源取得及為電腦安裝修補程式。
- 為您的電腦安裝個人防火牆、間諜防護及病毒檢測軟件，並定時檢測在電腦內任何的入侵、間諜軟件及病毒。同時，為該類檢測的軟件啟動自動更新間諜及病毒定義檔的功能。
- 避免下載或安裝來歷不明的程式、檔案或電子郵件。
- 取消瀏覽器內「自動完成」的功能。該功能在啟動後能記錄您所輸入的資料（包括網上密碼）。
- 不應共用電腦。如必須共用，應設定您的個人密碼以防止他人使用您的電腦賬戶。
- 在每次使用後，應中斷與互聯網或手機應用程式的連接。

如您懷疑:

(1) 曾登入可疑的網上證券或開啟偽冒電郵，並提供個人資料或進行交易，

(2) 您操作網上證券服務及 / 或流動網絡證券服務之密碼已外洩、遺失或被盜用，

(3) 賬戶有任何異常或未經授權的操作，

請盡快通知本公司。

四、 常見的網上詐騙活動

預繳費用詐騙案

這類詐騙案，涉及來歷不明的人士發出的信件或電郵，聲稱收件人只需協助處理一筆鉅款，即可獲得厚酬。訛稱涉及的款項，可能是公司利潤、賄款、未動用的政府經費、或是已故人士未領取的款項等。有時，為說服收件人該筆筆款項確實存在，便聲稱只需登入某個銀行網站（實質是虛假網站），便可看到有關戶口，顯示存有大額結餘。

這類交易，一般要求收件人先付一筆費用，以便完成交易。但是，該筆款項會從此消失，永遠無法追回。另外，收件人的個人及銀行資料，也有可能被利用， 作其他詐騙活動的工具。

網上博彩詐騙案

這類詐騙案，涉及來歷不明的人士發出的信件或電郵，假裝收件人已中了彩池。信件內容，會要求收件人提供個人及銀行資料，甚至會要求收件人繳付一筆手續費，才可領獎。待受害人付出款項，款項就會從此消失，永遠無法追回。另外，收件人的個人及銀行資料，也有可能被利用作其他詐騙活動的工具。

網上騙案層出不窮，請客戶加倍留意及小心保管個人及銀行資料。

如懷疑受騙，或遇到疑似騙案，請報警求助！