Security

1. Internet fraud and phishing

Phishing, the practice of using fraudulent e-mails and copies of legitimate websites to extract financial data and other personal information from unsuspecting computer users, continues to expand in sophistication and customers of financial institutions are increasingly targets of these scams. Because phishing materials often look genuine and may appear to originate from real people, organizations, institutions, and websites, the following precautions are suggested:

1.1 E-mail precautions

- Be cautious about clicking any links, opening any attachments, or downloading any files from e-mails regardless of file type or who sent them.
- Never open a website using a link provided in a suspicious e-mail. Links and the e-mail sender address can be forged.
- Avoid including sensitive personal information in e-mail messages. A better practice is to call a company directly.
- Be wary of any request that asks you to perform an urgent action (e.g., “Security Check”, “Activation”, “Verification” or any request to wire funds or make other payments).

1.2 Online banking and financial services precautions

- Always type the official website address (URL) when logging into a financial institution.
- When logging into the website, check for a letter ‘s’ immediately after the “https” prefix and for the closed lock icon at the right-hand bottom of the screen. The URL line must be green, lock sign closed and “Sberbank (Switzerland) AG [CH]” must be clear visible This indicates that both the site and connection are encrypted.
- Be wary of any request that asks you to disclose or verify information about yourself or your accounts, in particular, passwords or other information that a financial services provider may use to identify you (e.g. date of birth, mother's maiden name).

1.3 Computer system precautions

- Keep computer software (e.g., system patches, anti-virus, and anti-spyware) up to date with the latest security patches.
- Contact the relevant institution immediately if you notice anything irregular with your bank account or other online accounts.
- If your computer and/or internet connection appear erratic or crash unusually during an online banking session, disconnect the session and contact your bank’s support desk for assistance.

2. Unsolicited communications

- E-mail fraud is a common way that thieves attempt to steal your information. Here are some examples of methods used:
- Illegitimate offer e-mails advertise the sale of items at a reduced or even unrealistic price in order to obtain credit card or other financial information. Usually, the purchased products are not delivered.
- Requests for assistance scams usually offer the recipient large sums of money in exchange for financial assistance. A common example involves requesting a user’s bank account information in order to facilitate a deposit into the user’s account. This information is then likely used for fraudulent purposes.
- Phony sender e-mails purport to come from executives of an organization (e.g. John Doe, CEO). These e-mails often request personal or confidential information and may contain a

SBERBANK

"special" offer in order to solicit a response.

When contacting a financial institution or sender to verify a request for information, use only a phone number that comes from a reliable source (e.g., the back of your bank card, the phonebook, or bank statements).

Sberbank (Switzerland) AG will periodically contact clients through different channels such as e-mail and phone, but will never request that the client provide their electronic banking credentials on an unsolicited basis.

Spam messages are targeted, mass-distributed, unsolicited e-mails. These e-mails may contain offers to buy items, attempt to solicit your business, or invite you to visit a website. Unfortunately, while these offers may appear legitimate, many people have lost money responding to offers that are often fraudulent.

Here are some tips to help you avoid spam scams:

- Protect your information. Do not share any personal or financial information with unverified or questionable organizations or individuals.
- Question the provider. Know who the business is and its contact information.
- Time is on your side. Be wary of e-mails that implore you to "act immediately."
- Read the fine print. All contracts should be in writing and carefully reviewed prior to transmission of any payment.
- Be wary of free offers. Never exchange payment or financial information on order to obtain a free item. Never buy anything advertised in an unsolicited message.
- Be proactive in securing your data. It is advisable to periodically evaluate the risks that you face when conducting business online and take the appropriate steps to ensure that your business activities and data are safeguarded.

Contact Sberbank (Switzerland) AG when you notice any suspicious account activity or experience any information security related events.