How to Identify a Fraudulent Email

Identifying phony email messages is not always easy and the criminals who use them are becoming more sophisticated about creating them. Phony email messages may ask you to reply directly or select a link that takes you to a fraudulent website that appears legitimate. In either case, the messages will generally ask you to provide sensitive personal, financial, or account information.

Here are some tips for spotting fraudulent emails:

- **Urgent or threatening tone** — often, these emails claim that your account may be closed if you fail to confirm or authenticate your personal information immediately; Key will never send an email to a client to inform him or her of a problem with his or her Online Banking status, Debit/Credit Card account, potential fraud, or any other information pertaining to accounts
- **Request for personal or financial information** — fraudulent emails often claim that the bank has lost important security information that needs to be updated; they also may request that the user visit and update this information online and link you to a counterfeit website
- **Misspellings and poor Grammar** — fraudulent emails often use improper grammar and contain misspellings

General Precautions

- Delete suspicious emails without opening them; if you do open a suspicious email, do not open any attachments or click on any links in the email
- Never click on links from suspicious or unknown senders
- Do not launch email attachments from an unknown sender
- Never log into your account through a link provided in an email, even if it looks like it is coming from Key or a company you deal with regularly; instead, open a new browser and type the known Internet address for Key or the company in the address bar

- If you receive email from a known sender, do not launch an attachment without checking with the sender – even an email that appears to be from your computer manufacturer or a friend could be a fraudulent email containing a virus, Trojan horse, or worm
- Be selective when providing your email address to a questionable source; sharing your email address can make you more likely to receive fraudulent emails
- If you have been defrauded, report it to law enforcement authorities – many frauds go unreported, due to shame, guilty feelings or embarrassment
- Backup important files and when you aren✗t online, disconnect from the Internet; no computer is 100% secure
- Only do business with companies you know and trust
- Only enter your credit card information on sites that have the "lock" icon at the bottom of the browser and "https" preceding the URL