Protecting your privacy and confidentiality as a candidate.

Beware of Recruiting Scams

There are known incidents of recruiting scams whereby fraudsters attempt to take advantage of job seekers by pretending to be employees or representatives of well established companies, such as KeyBank. Using various methods (e.g., offering jobs that are too good to be true then asking for banking information, or gathering personal information via fraudulent employment applications), they seek to entice unsuspecting job seekers to pay money or to disclose sensitive personal or financial information.

Please note that KeyBank will never ask for money or payment from candidates, or request bank account information at any point in the recruitment process.

Potential Signs of a Scam

The following common red flags could help you identify whether the communication you received is a scam:

- Communications come from a free email-account such as through Gmail, Yahoo or Hotmail.
- Communications are unsolicited and you may not even recall having applied or provided your resume to the company or website referenced.
- They ask to schedule an interview via an online chat room, such as Google Hangout or Yahoo Messenger.
- There is urgency in their interest in scheduling an interview or they offer you a job "on the spot." The job offer is too good to pass on (e.g., offer a high salary, the ability to work from home, or employment visa sponsorship).
- They ask for sensitive personal information (e.g., gender, date of birth, or Social Security number).
- They ask for banking information often saying that it is required for the hire process, or for payroll processing.
- They ask for money (e.g., requests to wire funds to a bank account) as part of the application, hiring process or to cover visa sponsorship fees.

How to Report a Scam

If you think that a communication that you received from someone claiming to be a KeyBank representative or employee may not be legitimate, please do not interact or provide any information. Instead, please report the incident as follows:

- Forward suspicious emails to emailfraud@keybank.com (please **do not change or re-type the subject line**, as this may inhibit our ability to investigate).
- Report the scam to the Federal Trade Commission.

- If you are a KeyBank client and provided your banking information in an online interview, immediately contact Key's Fraud & Disputes Hotline at 800-433-0124.
- If you are not a Key client and provided your banking information in an online interview, contact your bank immediately.

Visit KeyBank's Privacy & Security page for more information.