From: J.P. Morgan
To: Program Administrators
Subject: Tips to protect your organization against executive impersonation scams

We invest heavily in cybersecurity capabilities to reduce the impact and inconvenience of fraudulent activity for your organization. As we continuously monitor trends in fraud, we want to make you aware of one of the latest forms of fraud threatening organizations of all sizes: Executive Impersonation.

What is Executive Impersonation?
- The fraudster spoofs an executive’s email account or pretends to be an executive on the phone.
- Specified emails may be targeted to individuals who can provide information or initiate payments.
- Fraudsters can perform a significant amount of research on the targets and the company to support their scheme beforehand.
- Types of scams include (but are not limited to): Requests to purchase gift cards, irregular wire transfer requests, and checks.

Tips to protect your organization:
- Carefully scrutinize all emails.
- Be wary of irregular emails that are sent from senior executives, as they are used to trick employees into acting with urgency.
- Review emails that request information/funds to determine if they are out of the ordinary.
- There are a few red flags you can look out for:
  - The email address contains a suspicious domain.
  - The sender name is vague, the content contains poor grammar, or includes an irregular link (different from your organization’s standard email address).
  - A caller claims to be an executive working for your organization, ask them politely for their internal phone number and say you’ll call back.

More information
- For additional ways to protect your business, check out the following information:
  - Payments Fraud Hits Record Highs
  - Check Fraud & Business Email Compromise (BEC) Scams Are on the Rise
  - GSA SmartPay® 2 clients, please call: 1-800-207-5359
  - U.S. and Canadian clients, please call: 1-866-725-1184

Questions:
- If you have any questions, please contact your program coordinator:
- U.S. and Canadian clients, please call: 1-800-207-5359
- GSA SmartPay® 2 clients, please call: 1-866-725-1184

DO NOT REPLY: Replies to this email will not be read or responded to. To contact J.P. Morgan, please do not reply to this email, but instead contact your relationship manager or program coordinator.

ABOUT THIS MESSAGE:
- The service message was sent to you as a J.P. Morgan customer to provide you with account updates and information about your J.P. Morgan relationship.
- Although this transmission and any attachments are believed to be free of any virus or other defect that might affect any computer system into which it is received and opened, it is the responsibility of the recipient to ensure that it is virus free and no responsibility is accepted by J.P. Morgan Chase & Co., its subsidiaries and affiliates, or applicable, for any loss or damage arising in any way from its use. If you received this transmission in error, you are hereby notified that any disclosure, copying, distribution, or use of the information contained herein (including any reliance thereon) is STRICTLY PROHIBITED. Please immediately contact the sender and destroy the material in its entirety, whether in electronic or hard copy format. Thank you.

View additional information on practices used by J.P. Morgan and how to safeguard your online activity at jpmorgan.com/info/jpmcpractices.

©2018 J.P. Morgan Chase & Co. All Rights Reserved. J.P. Morgan Chase Bank, N.A. P.O. Box 659752, San Antonio, TX 78265–9752, member FDIC. Operating in Canada through JPMorgan Chase Bank, N.A., Toronto branch, a Schedule III bank under the Canadian Bank Act. Authorized by the Prudential Authority and registered by the Financial Conduct Authority and the Prudential Regulation Authority. All services are subject to applicable laws and regulations and service terms. All trademarks, tradenames, and service marks appearing herein are the property of their respective owners.