WELLS FARGO

Treasury Management

Triumph over takeover: Steps to help protect against account takeover fraud

Account takeover fraud occurs when a fraudster obtains confidential information — including user IDs, passwords, PINs, and token codes — and uses it to access online banking accounts, transfer funds or commit other fraudulent acts. Fraudsters gain access by tricking you to divulge your online banking credentials or installing malicious software (malware) on your devices.

Use this checklist to help reduce your risk of account takeover fraud.

- ☐ **Beware of unexpected token prompts or on-screen messaging**
  The CEO® portal does not prompt for a token during sign on. If you see a token prompt during sign on, or if you are asked to enter your phone number or name during your CEO session, do not enter your information and contact us right away at 1-800-AT-WELLS (1-800-289-3557), option 2, or contact the service team who normally assists you.

  Most users see token prompts only when accessing high-risk payment services (such as Wires, ACH, Foreign Exchange) or administrative functions within CEO.[1]
- ☐ **Protect your credentials**
  Protect your RSA SecurID token and CEO Mobile token. Wells Fargo will never ask you for your token PIN, PIN + token code combination or Secure Validation code in phone calls, emails, or text messages.
- ☐ **Implement dual custody**
  Require all payments or user modifications initiated by one user be approved by a second user on a different device.
- ☐ **Require multi-factor authentication**
  Add a layer of protection by using multi-factor authentication (MFA) for accessing your company networks, including email, and for payments initiation.
- ☐ **Never click on links from unknown senders**
  Links and attachments in emails and text messages are a common way to deliver malware. Never click on links or download attachments or install programs without verifying the sender.
- ☐ **Monitor accounts**
  Check your accounts daily to detect suspicious activity.
- ☐ **Sign up for alert services**
  Receive a text or email notification informing you of electronic debits from your accounts.
- ☐ **Update antivirus software**
  Reduce your risk of account takeover fraud by blocking infected links before you ever see them.
- ☐ **Initiate transactions from stand-alone PCs that do not allow email or web browsing**
  Limit the possibility of malware downloaded through links, pop-ups, or attachments.

If you suspect fraud, contact your banker or relationship manager immediately.

1 Users who are subject to the European Union's Payment Services Directive (PSD2) or the Hong Kong Monetary Authority's revised E-banking supervisory expectations are required to use a token code immediately after CEO sign-on.