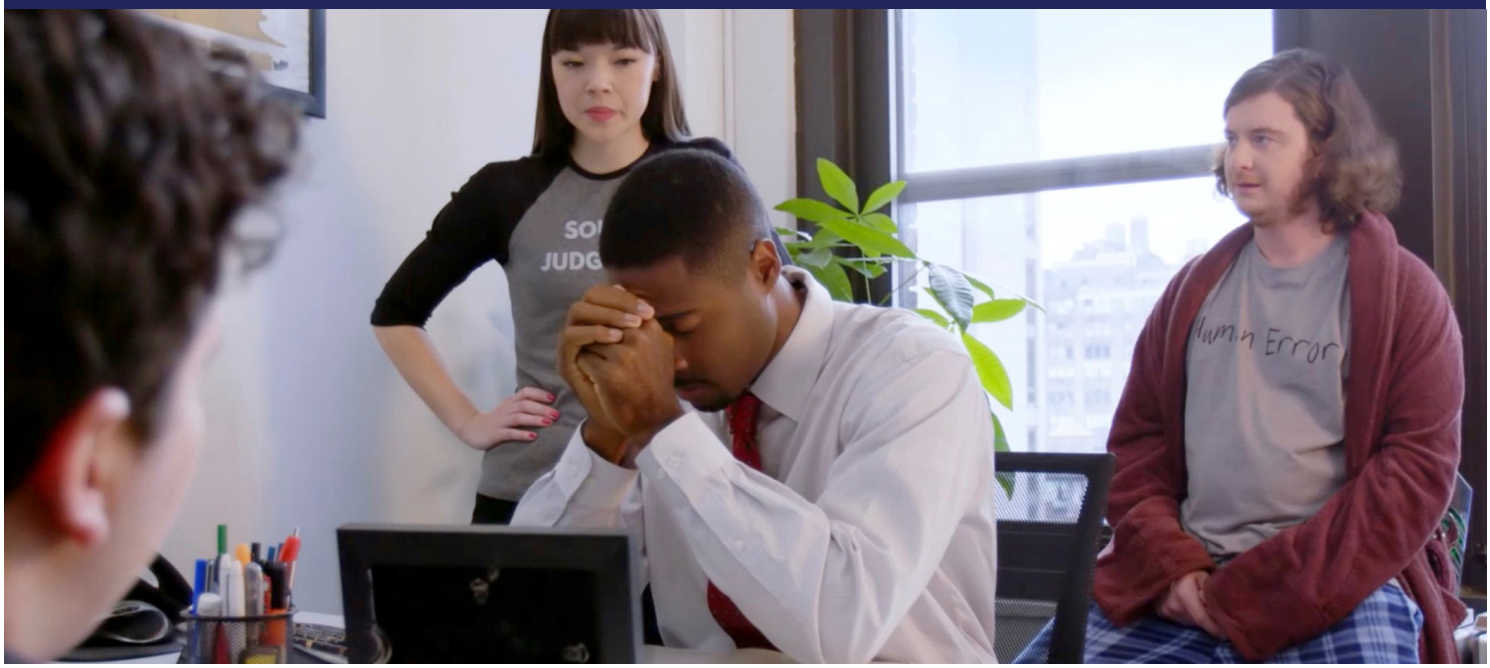

Wire Transfer Fraud

What you should know about it:

Reports of wire transfer fraud have soared from 14% of companies (2014) to 48% (2017).* Cybercriminals trick individuals into initiating fraudulent payments or providing information they can use to steal directly from company accounts. Wire payments are executed by the financial institution almost instantly. They can be impossible to reverse.

Criminals have become sophisticated about impersonating staff members to make urgent requests seem legitimate. For example, they've started linking wire scams to tax requirements, and using domestic accounts rather than more suspicious international accounts. Today, employees need to be more careful.

**2018 AFP® Payments Fraud and Control Survey*
Report, Association for Financial Professionals, 2018.

How to safeguard against it:

- **Always follow the company's processes for authenticating payment requests and making payments.**
- **Check personally with your manager or vendor before responding to any unexpected request for a wire transfer or other payment.**
- **Be suspicious of urgent requests and ones that are made at a time when it may be harder to confirm them.**
- **Carefully confirm any requested changes to a vendor's payment location.**
- **Don't be tricked by calls or emails, claiming to be from the IRS or other tax authorities, that demand immediate wire transfer payments.**
- **Avoid posting information on social media that might be used by fraudsters to impersonate you (for example, information about your travel plans).**
- **Contact company security immediately if you suspect someone is trying to commit wire transfer fraud.**