Fraud prevention tips and tricks

Fraudsters are constantly coming up with new ways of defrauding their victims. moneycorp is dedicated to preventing fraud and this includes ensuring that our customers are aware of potential risks and red flags to look out for.

In the 2018 Internet Crime Report, an annual report published by the FBI's Internet Crime Complaint Center (IC3), it was concluded that the greatest financial loss to internet crime came from Business Email Compromise ("BEC") and Email Account Compromise ("EAC"), which resulted in a loss of $1.298 billion from 20,737 victims in 2018.

How moneycorp helps prevent fraud

All staff is trained to identify potential red flags that could indicate fraud and to take appropriate steps to verify the transactions in question prior to moving forward. moneycorp also only accepts payment requests from authorized contacts from authorized email addresses. Lastly, we verbally verify all new banking instructions or changes to existing banking instructions received via email from our clients by making an outgoing call to an existing authorized phone number.

If a fraudulent payment occurs, moneycorp will do our best to recall the funds, however we cannot guarantee we will be able to get the funds back. Often, the fraudster will quickly withdraw the funds or transfer into another account and it becomes difficult or impossible to recover.

What you can do to prevent fraud

Always verbally verify new instructions received via email. If you receive new bank details or a change to banking details via email, it is crucial that you verify these details verbally with your payee.

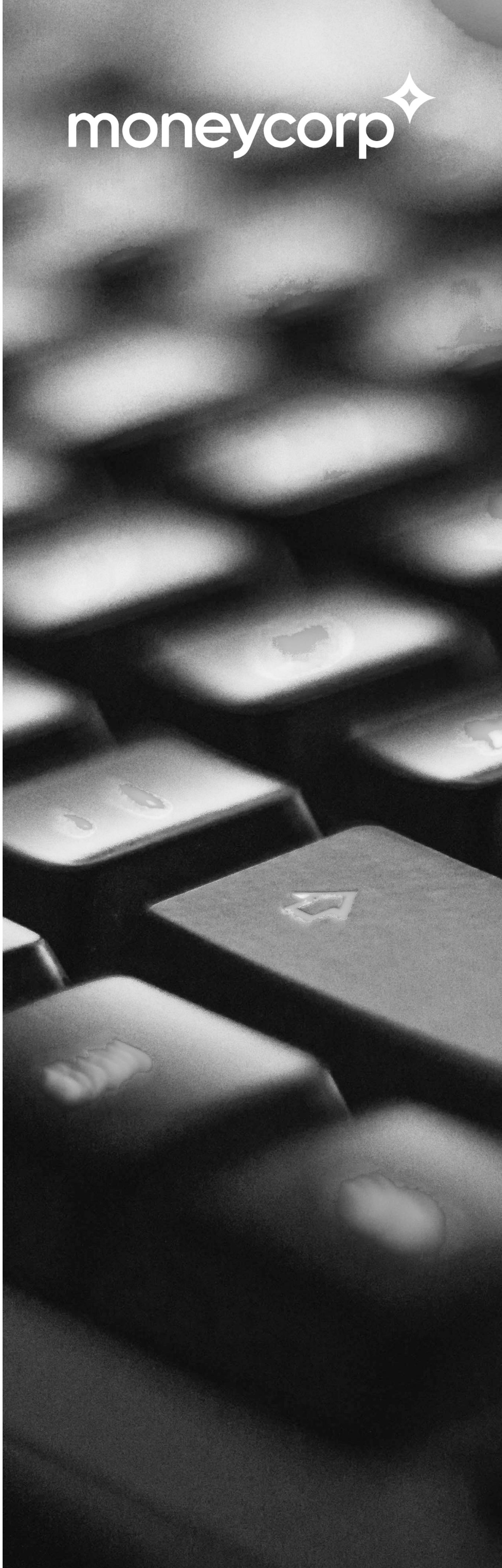
Look out for typical red flags in emails, which include, but are not limited to:

- Typos, misspellings, oddly worded emails.
- Slight changes in email domain from prior correspondence.
- Requests that pressure you to get things done immediately or without verbal verification.
- Banking instructions where the bank location and location of the payee do not correspond (i.e. the bank account is in a different country than the payee address).
- If an invoice was received, open it and look for any discrepancies or typos. Compare to past invoices from the same payee if you have them.

If you receive a phone call, either from an unknown number or a known number, and something sounds off, hang up and place an outgoing call to a known number for that individual.

Talk to your Account Executive about making sure your account information is up to date, including address, contact information, and authorized users.

If you enter payments online, do not share your username with anyone else and make sure to change password frequently.



moneycorp

Use this checklist to help mitigate any fraud risks at your organization.

Feel free to print and leave at your desk for a quick and easy way to take action if you become a victim of fraud. Additionally, you can send this checklist to your compliance department to ensure your entire organization has a reliable action plan.

Printable Checklist

What to do if you become a victim of fraud.

□ Change your email passwords and set up two factor authentication when possible.

□ Run a virus/malware scan.

□ Report the incident to your moneycorp Account Executive and include as much information as possible, including email correspondence, invoices received, etc. Your Account Executive will send this to moneycorp's Fraud department to conduct an investigation.

□ Report the incident to any other relevant financial institutions, the FBI's IC3 Division, or law enforcement as necessary and appropriate given the facts and circumstances of the incident*

□ Report the incident to your entire organization to prevent any further compromises due to fraud. Include important details such as who the email came from, any infected links, etc.

Have questions? Get in touch

Call 800 239 2389 or email contact@moneycorp.com

*We cannot get involved in reports our customers file to authorities unless otherwise contacted or compelled to do so by law enforcement or another government agency through appropriate channels. We have no insight into the internal risk controls of a client environment. What we can do is provide fraud education adn best practices to help clients against fraudulent transactions.