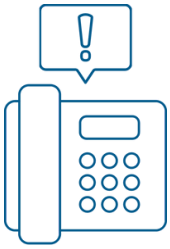
How to ID Potential Fraud Scams Quickly

MCKESSON

Be Watchful	Take this Action
 **Be prepared and alert.**	• Ensure staff is aware of procedures to respond to suspicious activity, including cybersecurity protocols. Regular training and awareness programs can help reinforce these practices. • Enable sales order notifications for accounts when possible.
 **Secure McKesson account access.**	• Verify all personnel have appropriate systems access according to their job role. • Notify McKesson of personnel changes impacting McKesson account access as soon as possible. • Never share passwords over the phone or email, even if the requester claims to be from IT support or a trusted entity. • Avoid requests for remote computer access unless initiated through official channels and confirmed by IT personnel with a valid support ticket.
 **If you receive a call asking for account information, login credentials or other private information.**	• Ask the caller for their name and phone number and hang up immediately. Then, promptly report the details to McKesson. • Contact your state's Board of Pharmacy using the number you have on file should you receive a call from a person stating they are the Board of Pharmacy. Most correspondence from the Board of Pharmacy will be via postal mail or email. • Protect your account information, McKesson login credentials, Medical license number and other privileged/private information. Do not share this information with anyone calling the practice. It is important to remember that a McKesson employee will never call you to request this type of private information.
 **If you receive a suspicious email or chat message asking you to click a link, open an attachment, respond with sensitive data or complete an unexpected request.**	• Hover over the links in the email (to see the true destination) and compare them to a legitimate site. • Call a known phone number (not one from the suspicious email/chat) and ask about the message. • Visit a trusted website by typing the address in your browser. • Promptly report details to McKesson.

Call or report suspicious activity through the McKesson Integrity Line at 1-877-625-4625 or at integrity.mckesson.com. For more information about how to avoid and report scams, go to the FTC Consumer Information site at https://www.consumer.ftc.gov/features/scam-alerts

How to ID Potential Fraud Scams Quickly

MCKESSON

Be Watchful	Take this Action
 **If you experience suspicious login activity or you are locked out of your McKesson ordering portal.**	• Reset your password immediately using your trusted systems password reset instructions. • Promptly report this to McKesson.
 **If there is suspicious order activity under your account.**	• Verify all orders on your McKesson ordering portal. • If fraudulent order activity is suspected, promptly report this to McKesson.
 **If a courier company other than your regular courier driver/company visits your site to pick up and process returns.**	• Release returns only with an approved Return Authorization from McKesson. • Only release returns to McKesson approved couriers. • Call McKesson immediately to report any variations in the returns process.
 **If you receive a suspicious invoice.**	• Do not remit payment until invoice is validated. • Validate invoice details with account purchase history. • Call a known phone number (not one from the suspicious invoice) and ask about the invoice. • If unable to validate, promptly report details to McKesson.
 **If you receive suspicious recall notifications.**	• Check your McKesson ordering system to confirm if the recall is listed. • If the recall is not listed in your McKesson ordering system, contact McKesson or the vendor directly using verified contact information on file.

Call or report suspicious activity through the McKesson Integrity Line at 1-877-625-4625 or at integrity.mckesson.com. For more information about how to avoid and report scams, go to the FTC Consumer Information site at https://www.consumer.ftc.gov/features/scam-alerts

How to ID Potential Fraud Scams Quickly

MCKESSON

Be Watchful

Take this Action

If you receive a suspicious wire transfer/banking change request.

- Do not complete transfer or make billing changes until request is validated.
- Call a known phone number (not one from the current request) to authenticate transfer/banking change.
- If unable to validate, promptly report details to McKesson.

Tips to prevent check fraud.

- Utilize online secure payment portals or electronic payment methods whenever possible.
- Secure checks in a locked and secure location with controlled access.
- Develop internal controls to separate the responsibilities of writing checks, reconciling accounts, and authorizing payments.
- Use high-security checks with features like microprinting, watermarks, and security threads.
- Use permanent gel ink to make it harder for threat actors to alter checks.
- For outgoing mail, use a post office or a secure drop box instead of regular mailboxes.
- Monitor financial accounts closely.
- If you suspect check fraud, notify your bank immediately and consider filing a police report.

Tips to prevent credential compromise.

- Keep operating systems and software updated with the latest security patches.
- Use strong unique passwords/usernames for each account and rotate regularly.
- Utilize a password manager where possible.
- Enable MFA (Multi-Factor Authentication) or SSO (Single Sign On) when able.
- Configure your browser to clear cookies & cache upon exit. If your browser does not support this, do so manually.
- Avoid downloading software from untrusted sources.
- Avoid entering credentials on pages reached through email links.

Call or report suspicious activity through the McKesson Integrity Line at 1-877-625-4625 or at integrity.mckesson.com. For more information about how to avoid and report scams, go to the FTC Consumer Information site at https://www.consumer.ftc.gov/features/scam-alerts