

## Don't fall prey to a scam

The American Bankers Association and FDIC report that check fraud is one of the most common methods used today for scammers to take your money. As a company who issues hundreds of thousands of checks to providers, facilities, members and employers, it is easy for scammers to duplicate one of our checks and try to present it as their own.

Employer Driven Insurance Services, Inc. (E.D.I.S.) utilizes security measures such as positive pay to help catch and prevent fraudulent checks from making it through our bank. However, this means that if you receive a fake or counterfeit check which appears to be from E.D.I.S. and you cash or deposit the check, **you will be responsible for paying the money back to the bank or facility who handled the transaction for you.**

If you have received a check from E.D.I.S. that you were not expecting, ask yourself a few questions:

1. Are you insured through your employer, spouses employer or parents employer by E.D.I.S.?
2. Are you a provider or physician who provides medical, dental or vision services?
3. Do you have any reason that you would be receiving a check in relation to group medical, dental or vision insurance?

If the answer is no to the above, chances are you have a fraudulent check. If you are unsure and don't want to be responsible for paying the bank for cashing a fraudulent check, please call us at (888) 886-7973 and we will let you know if the check is good.

### How to Spot a Fake Check

Determining whether a cashier's check or bank check is legitimate is difficult just by physical inspection. However, there are some things you can do to help identify a fake check:

- Make sure the check was issued by a legitimate bank. While some counterfeit checks will include a legitimate bank's name, a fake name is a sure giveaway. FDIC [BankFind](#) allows you to locate FDIC-insured banking institutions in the United States.
- Check with the bank that supposedly issued the check to make sure it is real. Make sure you look up the phone number on the bank's official website and don't use the phone number printed on the check (that could be a phone number controlled and answered by the scam artist). Next, call the official number and ask them to verify the check. They will likely need to know the check number, issuance date, and amount.
- Consider how and why you received the check. If someone you don't know initiated the payment, be skeptical and proceed cautiously. Scammers often communicate with their victims via e-mail or text message. Their communications may contain poor grammar and spelling errors.
- Look where the check was mailed from--if the postmark is not the same as the city and state of the "supposed" issuing bank, it might be an indication the check is fake. Be especially cautious if it was mailed from outside the United States.
- Determine if the amount of the check is correct and as expected. Fake checks are often made out for more than the agreed upon amount. This is intended to coax the person receiving the check into wiring the overpayment back to the scammer.
- Official checks usually contain watermarks, security threads, color-changing ink and other security features. While scammers are able to sometimes copy these security features, the quality is often poorly executed.

## **What to Do If You Are Scammed**

If you think you've been targeted by a counterfeit check scam, report it immediately to any of the following agencies:

- The Federal Trade Commission at [FTC Complaint Assistant](#).
- The U.S. Postal Inspection Service at [www.uspis.gov](http://www.uspis.gov) (if you received the check in the mail).
- Your state or local consumer protection agencies. Visit [NAAG](#) for a list of state Attorneys General.
- For possible online crimes involving counterfeit checks and money orders, file an online complaint with the [Internet Crime Complaint Center](#) (a joint project of the FBI and National White Collar Crime Center).

In addition to notifying the bank whose name is on the check, you can notify the website or online service where you encountered the scammer (for example, the online auction website or job posting website), so they can block them from utilizing their services in the future.

For more help or information, go to [FDIC.gov](http://FDIC.gov) or call the FDIC toll-free at 1-877-ASK-FDIC (1-877-275-3342). Please send your story ideas or comments to [consumeraffairs3@fdic.gov](mailto:consumeraffairs3@fdic.gov)