Bank of Pontiac

www.bankofpontiac.com

FRAUD ALERT:

HOW TO AVOID ACCOUNT TAKEOVER FRAUD

What is an "account takeover"?

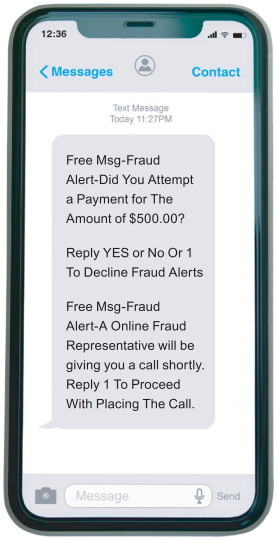
An account takeover happens when a fraudster poses as a financial institution to get your personal or account information. Once the fraudster has access to your account, they can make unauthorized transactions.

How Does It Work?

An account takeover begins with a fraudster sending a text message to your mobile phone. They usually claim they're from Bank of Pontiac's fraud department. They ask you to confirm a suspicious payment that was sent from your account - this may not be true and could be part of the fraud.

If this is a fraud attack, the fraudster typically follows up with a phone call and asks for your personal information to "cancel the payment." NOTE: Bank of Pontiac will NEVER ask for your personal information over the phone.

The account takeover fraud usually begins on a Friday, after business hours, and runs through the weekend.



How Can You Prevent Account Takeover Fraud?

If someone posing as Bank of Pontiac contacts you by phone, email, or text message and wants you to share your personal information, consider it fraud.

If you receive a text (or email) like the one shown here, do not reply to the sender. Ignore the message and do not call any phone numbers listed in the text.

If you receive a phone call that seems to be a phishing attempt, end the call immediately. And be aware that area codes can be misleading: a local area code does not always guarantee that the caller is local.

If you feel you have been the victim of fraud, please immediately contact Bank of Pontiac at 855-844-6151.

The phone (above) shows an example of a fraudulent "account takeover" text message.

AVOID FRAUD: Do not share your personal information with anyone posing as our institution.