First Midwest Bank
BANK WITH MOMENTUM

IDENTITY THEFT/ACCOUNT TAKEOVER FRAUD INFORMATION FOR PERSONAL BANKING CLIENTS

Identity Theft/Account Takeover - How does this happen?
This type of crime occurs when a thief obtains personal and banking information and intends to act as you to remove funds from your account, obtain credit in your name and live a lavish lifestyle. This can happen when information is obtained through theft of purses, wallets, home invasions, business theft, cyber attacks or trickery.

A loan application, opening a credit card, opening of a new checking account or purchasing of a home have all been exploited by thieves using other people's stolen personal information. Identity theft can be difficult to recover from depending on the circumstance. In some cases, the identity thieves use personal information for a short period of time or a one-time occurrence. Other times, the personal information can be used over and over again making the experience for the victim difficult.

The key to minimizing your risk regarding identity theft is to protect your personal information. First Midwest Bank has monitoring systems and employees that are trained to identify suspicious transactions and banking activity.

Listed below are examples of the methods and types of persons that perpetrate this type of fraud.

Methods of Theft

- Stolen purse or wallet
- Information stolen from dumpsters or trash cans
- Unsolicited phone calls, email and texts, or web sites used to trick the victim into giving personal and banking information (also known as social engineering)
- Theft of mail
- Internal theft from businesses holding personal information
- Malicious software that steals information from your computer
- Cyber attacks against public websites or other systems that have personal information

Who are Thieves?

- Anyone with malicious intent
- Professional identity thieves
- Family members or anyone who may have access to your home, online accounts or other locations of critical information

Indicators That You May Be A Victim

- Unauthorized charges on your checking account
- Unauthorized transfers or withdrawals on your bank statement
- Bills or credit card statements that don't arrive when expected
- Calls from financial institutions or debt collectors regarding accounts you did not open
- Accounts on your credit report that you did not open
- Receiving cards or billing statements from accounts you did not open
- Contact from companies about merchandise or services you did not buy

MORE PRECAUTIONS CONTINUED ON THE NEXT PAGE

First Midwest Bank
BANK WITH MOMENTUM

IDENTITY THEFT/ACCOUNT TAKEOVER FRAUD INFORMATION FOR PERSONAL BANKING CLIENTS (continued)

Protecting Yourself

- Don't click on links or attachments to unsolicited or unexpected email, even if it claims to be from friends or family
- Don't use the same password for multiple websites
- Enable online banking account and transaction alerts
- Be aware of when, why and to whom you give out your personal information
- Don't confirm or provide personal information in response to an unsolicited phone call, email or text
- Review account statements regularly or review account activity on-line
- Contact your bank for any discrepancies on your account
- Immediately report lost or stolen purses, wallets or checks to the bank
- Secure your checks, passwords, banking and other critical information
- Shred important documents containing account numbers, social security number, or other sensitive information
- Mail your bills using a post office box rather than curb side mailbox
- Review your free credit report from each of the credit bureau agencies each year
- Consider a credit monitoring program
- Consider placing a credit freeze with each Credit Bureau (see the web links below for more information)

Contact these websites for further guidance or if you believe you are a victim of identity theft

- www.consumer.ftc.gov/topics/identity-theft
- www.annualcreditreport.com
- www.transunion.com
- www.experian.com
- www.equifax.com

Visit FirstMidwest.com/Safe for the most current resources on a wide array of information security topics.