



# Protect Yourself from ID Theft

Identity thieves exploit the personal information and identities of millions of Americans every year. Compromised personal and sensitive information can be used to commit fraud or other crimes that can cost you time, money and potentially destroy your credit. First Bank of Highland Park is committed to protecting the security of your personal and sensitive information.

## Please be aware that First Bank of Highland Park will never:

- Require you to enter personal and sensitive information directly into an e-mail or other non-secure webpages
- Ask you to confirm, verify, or update your account, debit/ATM card or billing information via e-mail
- Send “threatening e-mails” stating to close or suspend your account if you do not take immediate action by providing personal information

## Keep your eyes open and don’t fall prey to fraud scams:

- Don’t give away personal information over the phone or online
- Keep identity documents, such as birth certificate and social security card, in a safe or locked filing cabinet
- Beware of claims that require immediate action or instill a sense of fear
- Beware of offers that require you to wire money or send a pre-paid card
- Do not open emails or email attachments unless the email was expected and verified
- Trust your gut – if you feel something is wrong, or an offer sounds too good to be true, it probably is fraud

## Steps to Consider for Protecting Yourself Against Fraud:

- Monitor your existing credit card and bank accounts closely for changes you do not recognize
- Shred all financial documents and other confidential information before discarding them
- Request and review your free credit reports by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228
- Create strong passwords with at least 10 characters using a mix of alpha-numeric characters (A, b, 1, 99) and symbols (\$, %, \*); do not use the same password for two critical websites or online accounts
- Protect postal mail by monitoring postal mail closely and act quickly if bills don’t arrive when expected or if a “new credit card” or account statement arrives; ask the post office to hold mail if traveling for a long period of time
- Place a credit freeze with the 3 major credit Bureau’s if you don’t intend on opening up new credit accounts or loans in the near future

## What should you do if you are a victim of identity theft?

- Report it to your local police and ask them to issue a police report. Keep a copy of it to share with your creditors.
- Document all correspondence pertaining to the incident
- Review your credit report and look for unauthorized changes and/or new credit lines
- Contact your creditors, financial institutions, utility and service providers to let them know you are a victim of identity theft
- Contact the IRS if you think your identity has been used in connection with tax violations
- Contact the postal service to see if anyone has submitted a change of address form on your behalf
- Place a credit freeze with the 3 major credit Bureau’s to prevent further fraud or unintended changes to your credit file
- Contact the fraud department at one of the major credit bureaus, Equifax, TransUnion, or Experian, to place a fraud alert on your file. One bureau will notify the other two of the flag on your credit.

If you believe you have been the victim of phishing or have any additional concerns, please contact your Personal Banker or Lender immediately. For additional information, visit First Bank of Highland Park’s Identity Theft Protection page at [www.firstbankhp.com/identity\\_theft\\_protection.aspx](http://www.firstbankhp.com/identity_theft_protection.aspx).