KCSB
KALAMAZOO COUNTY STATE BANK
YOUR JOURNEY. YOUR BANK.

When Information Is Lost or Exposed

Did you get a notice stating your information was exposed in a data breach? Did you lose your wallet? Did your online account get hacked? Or did you learn someone tried but failed to use your information to open an account? You could be at risk for identity theft. That's when someone uses your information – like your Social Security number or credit card – without your permission. Armed with information, an identity thief may open new credit or financial accounts, buy cars, apply for loans, online purchases, obtain Social Security benefits, rent an apartment, set up utility and phone service IN YOUR NAME.

If someone has already used your information to open a new account or make a purchase: Report it to the Federal Trade Commission (FTC) at www.IdentityTheft.gov (or call 1-877-ID-THEFT) and create an individualized recovery plan, based on the type of information exposed.

If an Identity thief hasn't misused your information yet: You don't need to file an FTC Identity Theft report. Keep reading to find out what you can do to help protect yourself from identity theft.

What can you do?

1. Deposit mail at a Post Office, a U.S. Postal Service collection box, or give it directly to your carrier.
2. Shred or tear up unwanted documents that contain personal information before discarding them.
3. **NEVER** give personal information over the phone or online unless you initiated contact. The Internet offers a convenient way to conduct business. To ensure you use it safely, never input your credit card or other financial (checking) account numbers at a website unless it offers a secure transaction. A secure (or "encrypted"" transaction will have these two features:
    a. An icon of a lock appears in the bottom strip of the Web browser page.
    b. The URL address for the Web page changes from "http" to "https" for the page at which you input the personal data.
4. Report credit card fraud to one of the major credit reporting agencies either online or by phone.
5. Report lost or stolen credit cards to the issuer immediately.
6. Memorize your Social Security number and passwords; don't carry them with you. Don't use your date of birth as a password.
7. Don't leave receipts behind at ATM's, on counters at financial institutions, at gasoline pumps or restaurants.
8. Check expiration dates on credit cards and contact the issuer if you don't get a replacement before they expire.
9. Monitor monthly bills and check financial statements for accuracy.

Key steps to help protect yourself from identity theft

1. Check your credit report to see if an identity thief has used your information:
    a. Get your free credit reports from www.annualcreditreport.com or call 1-877-322-8228 to request by phone.
    b. Review the reports and if you see an account or debit you don't recognize, contact the company and ask about it. If someone used your information to open a new account or make a purchase, report it to the FTC at www.IdentityTheft.gov and learn how to dispute the information on your credit report.
    c. Keep checking your credit reports periodically at www.annualcreditreport.com to watch for anything you don't recognize. You can check your reports online every week for free.
2. Freeze your credit to make it harder for someone to use your information. A credit freeze keeps people from getting into your report. While a freeze is in place, no one can open a new credit account. It's free to place the freeze, or to temporarily lift the freeze if you need to apply for new credit.

    Experian.com/help
    888-EXPERIAN (888-397-3742)

    TransUnion.com/credit-help
    888-909-8872

    Equifax.com/personal/credit-report-services
    800-685-1111

3. You can also place a free, one-year fraud alert by contacting one of the three credit bureaus. A fraud alert makes it harder for someone to open a new credit account in your name because a business must verify your identity before it opens the account.
4. Accept free credit monitoring if a company offers it due to a breach. Credit monitoring services scan activity that shows up on your credit reports. Depending on the service, it will usually alert you when something happens in your credit reports, like a company checking your credit, a new loan or credit card, or a company reporting a late payment.
5. If the event involved the U.S. Mail, report it to the US Postal Inspection Service.

    www.uspis.gov
    877-876-2455

6. Keep a record of the names and phone numbers of the people with whom you discussed your case and copies of all reports and supporting documents.
7. If you have been a victim of identity theft, you can file a complaint with the FTC by contacting the FTC's Consumer Response Center at 1-877-FTC-HELP (1-877-382-4357) or online at www.reportfraud.ftc.gov
8. If you have been a victim of identity theft, contact your local law enforcement agency and contact your bank. You may be advised to close your accounts. Be sure you change your PIN codes and passwords immediately.