Your info has been hacked. Now what do you do?

December 14 2014, byBrandon Bailey

In this Friday, Nov. 28, 2014 file photo, a shopper pays for her purchases at a Target store in South Portland, Maine. Criminals stole personal information from tens of millions of Americans in data breaches last year. Of those affected, one in three became victims of identity theft, according to research firm Javelin. (AP Photo/Robert F. Bukaty, File)

Criminals stole personal information from tens of millions of Americans in data breaches this past year. Of those affected, one in three may become victims of identity theft, according to research firm Javelin.

Whether shopping, banking or going to the hospital, Americans are mostly at the mercy of companies to keep their sensitive details safe. But there are steps you can take to protect yourself against the financial, legal and emotional impact of identity theft—and most of them are free:

AS A RULE:

— Closely guard your social security numbers—and those of your children—as well as credit and debit card information and account passwords.

— Shred unneeded financial records and credit offers.

DETECTIVE WORK:

— Examine credit card bills for irregularities each month.

— Get a free credit report once a year from at least one of the major reporting agencies (Equifax, Experian, TransUnion), and review it for unauthorized accounts. Ignore services that charge a fee for credit reports. You can order them without charge at www.annualcreditreport.com . If you order from each agency once a year, you could effectively check your history every four months.

DO PAID SERVICES WORK?

— Some experts say there's not much to be gained from a paid credit monitoring service. But if a business sends you a notice of a data breach, it can't hurt to sign up for any monitoring they offer for free. These services will tell you if a new account is opened in your name, but they won't prevent it, and many don't check for things like bogus cellphone accounts or fraudulent applications for government benefits. Some do offer limited insurance or help from a staffer trained to work with credit

issuers and reporting agencies.

SOMEONE STOLE MY IDENTITY, WHAT DO I DO?

— The Federal Trade Commission recommends immediately notifying one of the credit agencies and requesting a 90-day credit alert. (Each reporting agency is supposed to notify the others, but you may want to contact all three yourself.) The alert tells businesses to contact you before opening any new accounts in your name. You can renew the alert every 90 days, or you're entitled to keep it in effect for seven years if you've filed an identity theft report with police.

— Contact the credit issuer to dispute fraudulent charges and have the bogus account closed.

— Request your credit report and ask the reporting agencies to remove bogus accounts or any incorrect information from your record. Consider asking the reporting agencies to place a full freeze on your credit. This blocks any business from checking your credit to open a new account, so it's a stronger measure than a credit alert. But you should weigh that against the hassle of notifying credit agencies to lift the freeze—which can take a few days—every time you apply for a loan, open a new account or even sign up for utility service.

— Submit a report through the FTC website: www.consumer.ftc.gov . Click the "privacy & identity" tab, which will walk you through creating an affidavit you can show to creditors.

— Keep copies of all reports and correspondence. Use certified mail to get delivery receipts, and keep notes on every phone call.