When Information Is Lost or Exposed

Did you recently get a notice that says your personal information was exposed in a data breach? Did you lose your wallet? Or learn that an online account was hacked? Depending on what information was lost, there are steps you can take to help protect yourself from identity theft.

Is someone **using** your information to open new accounts or make purchases? Report it and get help.

What information was lost or exposed?

Social Security number

- [ ] If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
- [ ] Get your free credit reports from annualcreditreport.com. Check for any accounts or charges you don't recognize.
- [ ] Consider placing a free credit freeze. A credit freeze makes it harder for someone to open a new account in your name.
  - If you place a freeze, be ready to take a few extra steps the next time you apply for a new credit card or cell phone – or any service that requires a credit check.
  - If you decide not to place a credit freeze, at least consider placing a fraud alert.
- [ ] Try to file your taxes early — before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.
- [ ] Don't believe anyone who **calls** and says you'll be arrested unless you pay for taxes or debt — even if they have part or all of your Social Security number, or they say they're from the IRS.
- [ ] Continue to check your credit reports at annualcreditreport.com. You can check your reports every week for free.
- [ ] You might consider setting up an E-Verify account so you can lock your Social Security number at e-verify.gov/mye-verify.

  E-Verify is an online system that lets employers verify you're eligible to work in the United States, while also letting you lock your Social Security number so others can't use it to get a job. It's run by the U.S. Department of Homeland Security and the Social Security Administration. When someone tries to use a locked Social Security number to get a job, employers that use E-Verify must get more information from the person trying to use your Social Security number.

Online login or password

- [ ] Log in to that account and change your password. If possible, also change your username.
  - If you can't log in, contact the company. Ask them how you can recover or shut down the account.
- [ ] If you use the same password anywhere else, change that, too.
- [ ] Is it a financial site, or is your credit card number stored? Check your account for any charges that you don't recognize.

Debit or credit card number

- [ ] Contact your bank or credit card company to cancel your card and request a new one.
- [ ] Review your transactions regularly. Make sure no one misused your card.
  - If you find fraudulent charges, call the fraud department and get them removed.
- [ ] If you have automatic payments set up, update them with your new card number.
- [ ] Check your credit report at annualcreditreport.com.

Bank account information

- [ ] Contact your bank to close the account and open a new one.
- [ ] Review your transactions regularly to make sure no one misused your account.
  - If you find fraudulent charges or withdrawals, call the fraud department and get them removed.
- [ ] If you have automatic payments set up, update them with your new bank account information.
- [ ] Check your credit report at annualcreditreport.com.

Driver's license information

- [ ] Driver's license lost or stolen? Contact the nearest DMV branch to report it. Find the office at usa.gov/state-motor-vehicle-services. The state might flag your license number in case someone else tries to use it, or they might suggest that you apply for a duplicate.
- [ ] Check your credit report at annualcreditreport.com.

Children's personal information

- [ ] Request a free credit freeze for your child. A credit freeze will make it difficult for someone to use your child's information to open accounts. To place a freeze, follow the specific instructions for each credit bureau:
  - Equifax.com/personal/education/identity-theft/freezing-your-childs-credit-report-faq
    1-800-685-1111
  - Experian.com/help/minor-request.html
    888-EXPERIAN (888-397-3742)
  - TransUnion.com/credit-freeze/credit-freeze-faq#freeze-other-minor
    888-909-8872
- [ ] Generally, children won't have credit reports — unless someone is using their information for fraud. To find out if your child has a credit report, ask each credit bureau to check its records. Each bureau has specific instructions for these requests:
  - Equifax.com/personal/help/article-list/-/h/a/request-child-credit-report
  - Experian.com/help/minor-request.html
  - TransUnion.com/fraud-victim-resources/child-identity-theft
- [ ] If a credit bureau has a credit report for your child, the credit bureau will send you a copy of the report. Use the instructions provided with the credit report to remove fraudulent accounts.
- [ ] Review the FTC's information on Child Identity Theft.

Were you affected by one of these specific data breaches?

Equifax

In July 2019, Equifax settled a lawsuit stemming from its 2017 data breach, which exposed the personal information of 147 million people. Under the settlement with the FTC, CFPB and state attorneys general, Equifax has agreed to spend up to $425 million to help people affected by the data breach. If you were affected, you may be eligible for benefits. Visit ftc.gov/Equifax to learn more.

Marriott's Starwood Hotels & Resorts

In November 2018, the Marriott International hotel chain announced a data breach had exposed the personal information of anyone who made a reservation at one of its Starwood hotels or timeshare properties on or before September 10, 2018. To learn more about the breach and free monitoring services for affected customers, call 877-273-9481.

Here are some additional steps you might want to take:

Because your debit or credit card information may have been exposed ...

- [ ] Check your credit report at annualcreditreport.com.
- [ ] Review your transactions regularly. Make sure no one misused your card.
  - If you find fraudulent charges, call the fraud department and get them removed. Also, cancel your card and request a new one.
- [ ] If you have automatic payments set up, update them with your new credit card number.

Place a fraud alert ...

- [ ] Place a free, one-year fraud alert by contacting one of the three credit bureaus.That company must tell the other two.

Consider a credit freeze ...

- [ ] A credit freeze restricts access to your credit report, making it more difficult for identity thieves to open new accounts in your name.
  - It's free to place or remove.
  - It lasts until you lift or remove it.
- [ ] Set it by contacting each of the three credit bureaus.