What to do next...

if you're notified that your personal information has been part of a cyber breach.

- Learning about a breach that might impact you? Do a web search about the news story to learn more and visit *ftc.gov, idtheftcenter.org,* and *krebsonsecurity.com.*
- Find out from the company what information was stolen. Even if they tell you that your stolen information was encrypted, the data is at risk.
- See if they're offering affected customers free credit monitoring and identity theft protection.
- But read the fine print before accepting free services. Companies often require those who accept freebies to also opt out of participating in future lawsuits or claims related to the breach.
- Document everything you do and everyone you talk to related to managing accounts of a breached organization.
- Change your password and PIN number on accounts at a breached company immediately. And if you used the same or a similar password elsewhere, change them.
- Check your credit history for accuracy at *annualcreditreport.com*. They're offering free weekly access through April 20th, 2022.
- Sign up for a credit monitoring service such as *Credit Karma* and *Credit Sesame.*
- Place a security freeze on your credit files at Equifax, Experian, and TransUnion.
- Set up your IRS, Social Security, and other government accounts online now, if you haven't already, which prevents fraudsters from doing it first.

Sources: Privacy Rights Clearinghouse, Consumer Reports, Forbes, ZDNet, Fulton Bank, ID Theft Recovery, IBM

- Set up two-step authentication on every online account that offers it.
- Do a web search for usernames you use now or have in the past. Log in and change any that show up.
- Log in and delete online accounts you don't use anymore. And check out as a guest when you make online purchases moving forward.
- If you spot fraudulent charges on a bill or statement, notifying the company immediately will, in most cases, release you from the liability for these charges.
- Install password manager software on your computers, tablets, and smartphones.
- Set up text or email alerts for activity on debit and credit card accounts. Review monthly bills and statements for accuracy.
- Seeing suspicious activity on a bank, online store, or credit card account? Dispute the charges, and request a new credit or debit card.
- If you are affected by a data breach, visit *IdentityTheft.gov* to learn more about warning signs that your identity has been stolen and how to protect yourself moving forward.
- Remember, cyber criminals are sophisticated, and cybercrime is complex. It takes, on average, seven months for a company to discover it has been breached. All that time, criminals have had access to the stolen data.

NTSC
NATIONAL TECHNOLOGY SECURITY COALITION