Tips for Consumers: What to do Post-Breach

Data breaches pose a potential risk to consumers in the form of identity theft, account takeover and fraud when personal and sensitive information is compromised. The following are tips for consumers to consider in reducing the risk or impact of data breaches.

Place a Security Freeze on Credit Reports

A security freeze protects against identity theft and the opening of fraudulent accounts with a consumer's personal information. It will block an institution or lender from accessing a report, unless a pre-set PIN is provided to "thaw" the report; a credit report may be thawed at a particular bureau for a period of time or for a specific lender. Consumers must contact each of the bureaus listed below to place a security freeze.

Note: Each of the credit bureaus will give or allow you to create a PIN to be used to thaw or unfreeze your report in the future. It is very important you do not lose or forget this PIN! It is recommended to store it in multiple locations with other important documents, including a safe deposit box or home lockbox, or in a password-protected format electronically.

Go to each of the following sites to place a security freeze and follow the instructions; record and protect the PIN:

- Equifax: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- Experian: https://www.experian.com/freeze/center.html
- Innovis: https://www.innovis.com/personal/securityFreeze
- TransUnion: http://www.transunion.com/securityfreeze

Some states charge fees to place a freeze, thaw or unfreeze a credit report; see the sites above for specific state details.

Place a Fraud Alert on Credit Reports

A fraud alert on credit reports requires potential creditors to contact the consumer and obtain permission to open new accounts or lines of credit. Consumers are allowed by law to report they are an identity theft victim and file a fraud alert (aka a "security alert") every 90 days; with proper documentation such as a police report, the fraud alert period may be extended to seven years.

If consumers contact one of the first three listed below, that bureau is required to contact the other two; consumers must contact the fourth bureau directly to place an alert.

- Place a fraud alert with Equifax: call 800.525.6285 or go here; or
- Place a fraud alert with Experian: call 888.397.3742 or go here; or
- Place a fraud alert with TransUnion: call 800.680.7289 or go here.
- Place a fraud alert with Innovis: call 800.540.2505 or go here.

Unless there is an extended fraud alert in place, make a reminder to renew the fraud alerts after 90 days.

Check Credit Report Annually

Consumers are entitled by law to a free credit report from each of the credit reporting bureaus once a year.

- Go to annualcreditreport.com or call 877.322.8228 and follow instructions to access the free credit reports.

The free credit report will show all lines of credit and other obligations, along with other public data. It will not show the FICO score; consumers may contact their financial institution or a credit card issuer to request the FICO score. It usually costs a fee to retrieve a FICO score.

It is recommended consumers check their report three times a year by pulling the report for one bureau every four months. Items to watch for are "new" or "re-opened" accounts and other suspicious activity.

Note: Consumers need to beware of other sites that try to sell a credit report or offer a "free" report if you agree to sign up for a subscription service – usually credit monitoring. Also, watch out for look-alike sites that are not real, like "freecreditreport".

Leverage Financial Institution Safeguards

Check with financial institution for these additional account protections:

- A security challenge pass-phrase that must be shared before any changes are made to account(s); restriction to only perform secure withdrawals or transfers to pre-specified accounts;
- Alerts the institution offers to monitor online or phone transactions, wire transfers, international transactions, new payees added to bill pay and address or profile changes to accounts;
- Account notes and travel protections if going on vacation, especially out of the country; account notes for active duty military on assignment overseas, that they are not stateside;
- Destroy sensitive documents via a cross-cut shredder or at an institution's free "shred event".

Protect Against Fraud Scams

- Practice email safety: don't click on links in emails or open attachments unless the email was expected and verified; confirm a message is legitimate by contacting the sender directly via pre-determined contact information;
- Be suspicious of email or phone requests to update or verify personal information;
- Be wary of offers that are too good to be true, require fast action or instill a sense of fear;
- Be on guard against fraudulent checks, cashier's checks, money orders or electronic fund transfers with a request to return part of the funds via wire transfer;
- Use security and privacy settings on social network sites and beware of random contacts from strangers;
- Research "apps" before downloading, only download from an "app" store (iTunes, Play Store, Windows Store), and don't assume an "app" is okay because the icon resembles that of a bank;
- Beware of disaster-related scams where scammers claim to be from legitimate charitable organizations.

Protect Personal and Financial Information

- Review monthly bank and credit card statements closely and contact the financial institution immediately if any unknown transactions occur; better yet, if online or mobile banking is available for deposit and credit card accounts, make a habit of reviewing every few days to ensure immediate actions can be taken.
- Safeguard credit cards, social security numbers and other personal information:
    - Only provide sensitive information over secure websites or emails;
    - Do not provide personal information or log onto critically sensitive accounts (email, online banking, etc.) via public computers, like a hotel or library kiosk, or while using public WiFi.
- Wherever possible, utilize two-factor authentication to provide an additional layer of account logon protections; two-factor authentication requires two pieces of information to login to an account, usually the password and a code from an SMS text message or approving the login via phone call. To check whether a website offers two-factor authentication, check this site: https://twofactorauth.org.
- Use password protections:
    - Create long passwords with at least 10 characters and using a mix of alpha-numeric characters (A, b, 1, 99) and symbols (@, $, %, *);
    - Instead of a password, use a passphrase, a long (15-25 char) phrase or sentence that only makes sense to you and is easy for you to remember; do not use something common like "Maryhadalittlelamb." and use something uncommon like "MichaelWhassocceronThursdays.".
    - Use a password checker to verify the strength of the selected password; do NOT put a valid password into an online password checker; instead, use a variation that is similar but not the same;
    - Do not use the same password for two critical websites or online accounts, do not share passwords with others and do not use the "Remember My Password" feature in web browsers;
    - Unless you use a very long and difficult password, change passwords often; and
    - Use a password manager to enable longer passwords without having to write them down.
- Protect postal mail by locking the mailbox, if possible; monitor 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.
- Shred bills, bank statements, pre-approved financial solicitations and other confidential information before discarding them; check for local free "shred events" to securely dispose of documents.