consumer action

Education and advocacy since 1971

Data Breaches

State-of-the-art Ronald Reagan UCLA Medical Center in Los Angeles is ranked nationally in 15 adult and nine pediatric specialties. It has a 466-bed general medical and surgical facility with 23,508 admissions in the most recent year reported. It performed 10,988 inpatient and 15,855 outpatient surgeries. Its emergency room had 46,128 visits, and on July 17, 2015, the Center announced that hackers broke into its computer network and may have accessed sensitive information on as many as 4.5 million patients. This comes on the heels of a major breach of federal employee records, and a massive hack at health insurance giant Anthem Inc. affecting 80 million Americans this year.

What is a data breach? The Identity Theft Resource Center (ITRC) defines a data breach as an incident in which an individual's name plus a Social Security number, driver's license number, medical records or financial records (credit/debit card numbers included) is potentially put at risk because of exposure. This exposure can occur either electronically or in paper format.

Types of data breach: According to Privacy Rights Clearinghouse, there are four major types of breach:

- A breach involving your credit or debit card information at a retailer's point-of-sale terminal
- A breach involving another existing financial account
- A breach involving your Social Security number
- A breach involving your driver's license number or another government-issued ID

What should you do when personal information has been compromised in a data breach? Consumers should pay close attention to any notifications or letters they receive from financial institutions, credit card issuers, health care providers or merchants regarding a breach in which their personally identifiable information was exposed, says research company Javelin Strategy & Research. The firm revealed in their 2015 Identity Fraud Study that two-thirds of ID fraud victims in 2014 had received a data breach notification earlier in the same year.

Privacy Rights Clearinghouse says the first thing you should do when notified that your personal information was compromised is figure out what type of breach has occurred. This will dictate what steps you should take next.

The Consumer Financial Protection Bureau (CFBP) recommends that you take the following fours steps if you think your credit or debit card data was hacked:

1) Check your accounts for unauthorized charges or debits and continue monitoring your accounts.
2) Report a suspicious charge or debit immediately.
3) Submit a complaint if you have an issue with your bank or card issuer's response.
4) Know when to ignore someone contacting you to "verify" your account information by phone or email.

What if the breach involves an existing financial account? If the breach involves an existing checking, savings, money market or other deposit account, Privacy Rights Clearinghouse recommends that you take the following steps to reduce the risk of fraud:

1) Ask your financial institution to close your old account and reopen it with a new account number.
2) Carefully monitor your accounts online and, if offered by your institution, set up text or email alerts of activities.

3) If you become aware of any fraudulent transaction, immediately report it to the institution, and follow up by formally disputing the transaction in writing.
4) Be suspicious of any email or phone call that you might receive about the breach that requests personal information.

What if the breach involves your Social Security number? If the breach involves exposure of your Social Security number, a thief could use the information to open new accounts in your name. Although research firm Javelin Strategy & Research revealed in its report released in March 2015 that new account fraud hit a record low in 2014, it continues to be one of the most damaging types of fraud. Privacy Rights Clearinghouse recommends that if you receive notice that your Social Security number was compromised in a breach you should take the following steps:

1) Notify credit reporting agencies and immediately place a fraud alert on your credit report.
2) Order your credit reports and examine them carefully for signs of fraud.
3) Consider a security freeze. It provides the greatest protection from ID theft.
4) Be suspicious of any email or phone call that you may receive about the breach that requests personal information.

What if the breach involves your driver's license number or another government-issued ID? If the breach notification indicates that your driver's license or another government-issued ID was compromised, you should contact the agency that issued the ID and ask what they recommend. As noted by Privacy Rights Clearinghouse, you may be instructed to cancel the ID and obtain a replacement, or the agency may "flag" your file to prevent an imposter from getting a license or other ID in your name.

Know your rights: According to the National Conference of State Legislatures (NCSL), 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private and/or government entities to notify individuals of security breaches of information involving personally identifiable information. You can find a list of state laws at NCSL's website (www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

In addition to state law, federal law may require notice for certain types of data breaches. For example, the federal Gramm-Leach-Bliley Act requires financial institutions to adopt procedures to safeguard customer data and notify customers when there has been unauthorized access to it. The HITECH Act requires the Department of Health and Human Services (HHS) to issue rules defining how and when consumers are to be notified of a breach of protected health information. You can check to see if your medical provider has reported a data breach at the HHS website (www.hhs.gov/orc/privacy.hipa.adminstration.breachnotificationrule/).

Resources:

Chronology of Data Breaches (Privacy Rights Clearinghouse): www.privacyrights.org/data-breach

CFPB Issues Consumer Advisory on Industry's Data Breach (CFPB): www.consumerfinance.gov/newsroom/cfpb-issues-consumer-advisory-on-industrys-data-breach/

$16 Billion Stolen from 12.7 Million Identity Fraud Victims in 2014 (Javelin Strategy): www.javelinstrategy.com/news/1556/92/16-Billion-Stolen-from-12-7-Million-Identity-Fraud-Victims-in-2014-According-to-Javelin-Strategy-Research/

Data Breach Reports (ITRC): www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf

May 2014 Intersections Consumer Notification Guide (Intersections Inc.): www.intersections.com/library/Consumer_Notification_Guide_May%202014_Final.pdf

Federal Trade Commission ID theft hotline: 877-438-4338

Annual free credit reports: www.annualcreditreport.com

Consumer Action empowers low- and moderate-income and limited-English-speaking consumers nationwide to financially prosper through education and advocacy. Visit us online at www.consumer-action.org.