Protecting Your Personal Information Online

By City Attorney Mara W. Elliott

From shopping to paying bills, we conduct most of our personal business online. As consumers, we entrust online companies with protecting the confidential information we share on their platforms. When they fail, they have a duty under the law to inform anyone whose information has been compromised.

Unfortunately, that's not what consumer credit reporting agency Experian did when a security lapse led to the exposure of personal financial information of more than 30 million individuals, a massive data breach that has impacted more than 2 million Californians. That's why my Office sued on behalf of the People of the State of California to hold Experian and its affiliates accountable and to force Experian to notify victims of the breach. Our case is headed to trial in January of 2022.

A dark web data breach

Experian will make billions of dollars this year by aggregating and selling highly confidential consumer information, including Social Security numbers, email passwords, and mothers' maiden names. From July 2010 through February 2013, Experian sold access to its databases to a hacker – a teenager living in Vietnam posing as a Singapore-based private investigator. The hacker admitted he resold the information to more than 1,300 individuals on the dark web for millions, and pled guilty to a federal crime for which he served several years in prison.

Holding Experian accountable

Despite knowing of the breach for years, and despite assurances to Congress that it would inform consumers of the breach, Experian and its affiliates still have not notified consumers. This is a violation of California law that has left people vulnerable to identity theft and other crimes.

Our lawsuit seeks to compel Experian and its affiliates to:

- Notify victims that the security lapse occurred, so they can take action to protect their financial data;
- Provide credit-monitoring and identity-theft protection services to the victims at no cost; and
- Pay fines and penalties as ordered by the court.

How to keep your data safe

Although consumers cannot control the actions of the companies that have access to their

(continued)

personal data, we can all take steps in our own lives to secure our information.

1) **Be diligent about cybersecurity best practices**

   Use strong passwords and update them regularly. Never allow your browser to save your password automatically. Instead, consider using password management software to establish and keep track of unique passwords for each of your accounts. You can also establish a two-factor authentication system for your most important accounts that prompts a second security verification through text or another application. Also, it is advisable to restrict the personal information you share on social media. Finally, be sure to download the latest security updates to your phone and computer and regularly clear your 'cache,' which can include saved cookies, searches, or other identifying information.

2) **Use your smart phone when making purchases**
   Most mobile apps require an additional identification step such as biometric fingerprint. This second verification adds an additional layer of security to the transaction.

3) **Don't fall for phishing**
   Phishing is an attempt to obtain personal information through deceptive texts, emails, or other communications. Often the sender pretends to be from a well-known company or organization. Red flags for phishing include misspellings and grammatical errors, links to unfamiliar websites, or bizarre email domains. Don't click on or respond unless a communication comes from a known source.

4) **Guard your browsing history and turn off ad personalization**
   Our browsing histories and online interactions provide companies with information about who we are – our finances, health, religious beliefs, consumer habits, and so much more. This information is used to tailor the online advertisements we encounter. Software is available that blocks these ads and the data they capture. You can also go into you the privacy settings on your devices and turn off ad personalization.

Consumers have a right to privacy and online safety. If you believe you have been a victim of online theft or fraud, please contact the Affirmative Civil Enforcement Unit of the City Attorney's Office at (619) 533-5618. Complaints may also be filed online, by filling out the ACE Complaint Form here:
https://www.sandiego.gov/cityattorney/divisions/civillitigation/civilprosecution

###

City Attorney Mara W. Elliott
1200 Third Ave., Suite 1620
San Diego, CA 92101
Phone: 619-236-6220
Email: cityattorney@sandiego.gov
www.Sandiego.gov/cityattorney