Thanks to John Metcalf, a member of the SCV Computer Club, for forwarding this information from LA Metro's Forensic Technology Manager.

You will find information about the breach via the below link plus how to check to see if your information has been compromised. https://www.equif axsecurity2017.com/

"Be careful everyone – news is out yesterday and fresh phish comes out today.

Remember to not open or click on emails and hot links you are unsure of, if it looks suspicious delete it, don't forward it.

Think before you click."

From: Equifax Security Team <Alert@equifax-notifications.com>
Reply-to: Equifax Security Team <Alert@equifax-notifications.com>
Subject: Official Data Breach Notification

EQUIFAX®

Dear Equifax Consumer,

As integrity is a primary concern of ours, we want to make sure you are aware of a recent data compromise that may have affected your personal information.

We have created a secure website for you to check if your information was involved in this compromise.

If you find that your information has been compromised, we are offering the ability to freeze your Equifax credit report as well as a free year of credit monitoring, to assist in protecting you from identity theft. Click here to take advantage of these offers.

Your trust is a top priority for Equifax, and we sincerely regret the inconvenience this may cause. The privacy and protection of your personal information is a matter we take very seriously and we are working diligently to resolve this incident.

Sincerely,

Equifax Credit Bureau

From Judy.....

Excerpt from Los Angeles Daily News article, 9/8/17

Has your data been hacked? Here's what you should do

From staff and wire reports

Equifax has set up the page equifaxsecurity2017.com so consumers can check if their data was stolen.

Here's what you can do if your information was stolen.

Consider putting a full freeze on your credit. This blocks any business from checking your credit to open a new account, so it's a stronger measure than a credit alert. BUT you should weigh that against the hassle of notifying credit agencies to lift the freeze — which can take a few days — every time you apply for a loan, open a new account or even sign up for utility service.

Check your credit card bill for any irregularities. Don't overlook charges, no matter how small. Thieves typically test a credit account by charging smaller amounts, usually under $10, to see if you notice. If you don't, they may charge larger amounts later.

Someone stole my identity. What now?

Contact the credit issuer to dispute fraudulent charges and have the bogus account closed.

Request your credit report and ask the reporting agencies to remove bogus accounts or any incorrect information from your record.

Submit a report through the FTC website. Click the "privacy & identity" tab, which will help you create an affidavit to show creditors.

Keep copies of all reports and correspondence. Use certified mail to get delivery receipts, and keep notes on every phone call.

How to avoid more hacks

After a hack, scammers may try to use the stolen data to trick you into giving up more personal information. They can use that info to steal money in your accounts or open new credit card.

Don’t click on any links from emails. Bad software could be downloaded to your computer that can steal account passwords.

You might get letters in the mail saying you won a tablet or vacation and give you a phone number to call. Don’t do it. It’s likely a ploy to gather more information from you.

Hang up the phone if you get a call asking for account numbers or other information. Scammers may also send texts, so don’t click on any links from numbers you don’t know.

The Associated Press contributed to this report.