NEWS FROM SCDCA

SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS

Carri Grube Lybarker, Administrator

Be on Alert in Wake of Facebook Breach

COLUMBIA, S.C. – The South Carolina Department of Consumer Affairs (SCDCA) is encouraging Facebook users to take action to secure their online accounts and guard against scams in light of the most recent breach announcement.

Over 90 million accounts were affected by the breach that gave access to consumers' personal data that can be used in phishing attempts or to answer security questions. Even if your account was not breached, scam artists follow the headlines and may use the breach in attempts to separate you from your personal information or money. Facebook users should consider the following to avoid falling victim to fraudsters:

- **Change your password and security questions**. Scammers could use your information to gain access to established accounts. Make sure security questions cannot be answered with information found on your Facebook account- ie: mother's maiden name, where you went to school or were married. Use strong, creative passwords (uppercase, lowercase and special characters) and don't share them with anyone. Don't use the same passwords or security questions for multiple accounts, especially when using your e-mail address as the login name on that site.

- **Watch out for phishing attempts.** Scammers often ask for personal or sensitive information via a phone call, text or e-mail. A fraudster may even use information gleaned from your Facebook account, like who your friends are or who you do business with, to make their phone calls, emails and other communications seem even more convincing. Never reply to calls, texts, pop-ups, or e-mails that ask for verification of personal information. Avoid clicking on links or downloading attachments from suspicious emails or texts. When fielding unsolicited communications of any type, know the red flags of a scam.

- **Take advantage of Facebook security options.** Access security options by going to Facebook's "Settings" on your computer or device. Next, go to "Security and Login." From this site you can: (1) Sign up for two-factor authentication, which requires an extra step to verify it's you attempting to log-in, (2) Get alerts when someone logs into your account from a device you don't normally use and (3) Check out the "Where You're Logged In" section and look for devices or locations you don't recognize and end suspicious sessions.

- **Consider what you share and who sees it.** Take stock of the personal information you share online. Once it's shared, it is difficult-or near impossible- to erase. Review privacy settings to see who can see your information and make any necessary adjustments.

– **Use antivirus or anti-spyware software and a firewall**. Make sure to update them regularly on your computers, smartphones and tablets. Phishing emails may contain software that can harm your computer or track your activities on the internet.

For more information on avoiding scams, see SCDCA's scam guide, "Ditch the Pitch." Scam reporting is an important step in helping SCDCA empower consumers to recognize and avoid scams. Report scams to SCDCA's Identity Theft Unit online or by calling 844-835-5322.

About SCDCA
The South Carolina Department of Consumer Affairs aims to protect consumers from inequities in the marketplace through advocacy, complaint mediation, enforcement and education. To file a complaint or get information on consumer issues, visit *www.consumer.sc.gov* or call toll-free, 1-800-922-1594.

###