LSC®
Helping Credit Unions Compete

Fraud Alert

Anthem Inc. February 23, 2015

On January 29, 2015, Anthem, Inc. (Anthem) discovered that cyber attackers executed a sophisticated attack to gain unauthorized access to Anthem's IT system. Anthem is a service provider to group health plans including Blue Cross and Blue Shield across the country.

Current or former members of one of Anthem's affiliated health plans may be impacted. In addition, some members of other independent Blue Cross and Blue Shield plans who received healthcare services in any of the areas that Anthem serves over the last 10 years may be impacted.

Anthem is working with the FBI's investigation and has retained Mandiant, one of the world's leading cybersecurity firms, to assist in the investigation.

For a listing of potentially impacted Anthem affiliated health plans and other Blue Cross and Blue Shield companies for which Anthem is providing this service, please see the Company's website:

www.anthemfacts.com

Anthem believes this suspicious activity may have occurred over the course of several weeks, beginning in early December, 2014. The following information is believed to been accessed:

Names
Dates of birth
Social Security numbers
Health care ID numbers
Home addresses
Email addresses
Work information like income data

The Company does not believe Credit card or banking information was compromised, nor do they believe medical information such as claims, test results, or diagnostic codes were accessed.

Although payment card information is not believed to have been compromised, Credit Unions need to make sure all processes and procedures are followed. The information accessed in the Anthem breach can result in fraudulent applications, account takeovers and various types of phishing scams.

- All Credit Unions should have internal procedures in place to validate the cardholder's identity prior to adding a travel indicator, changing limits or addresses for any existing credit or debit card. Phone numbers can be spoofed; do not rely on caller ID as part of your method to validate cardholder's phone numbers on the account. **Make sure to include out of wallet questions (pet's name, first car, favorite movie, etc.) as part of your validation process.**

- Phishing scams may also be attempted. Criminals will use email, telephone or text messaging to trick recipients into disclosing personal information.

Educating your members is key to reducing losses from phishing scams. Members need to know exactly how **phishing scams** work and how to avoid becoming a victim. Educating members that the Credit Union will *never* ask for your personal information via phone or email can be done on websites, online banking sites, newsletters, statement messages, or hold message.

1. Never respond to an e-mail asking you to verify or update your personal information

2. Never click on links in unsolicited e-mail that you receive

3. Delete any unsolicited email in your email accounts - don't even open them!

4. Never tell anyone your PIN and never write it down

5. Guard your PIN from being seen when you are completing a transaction at an ATM or in a store

6. Protect your passwords; never write them down or enter them online unless *you* initiated the transaction

7. Never give out personal or financial information over the phone or online unless you initiated contact

8. Check your credit report at least once annually or sign-up for weekly or monthly alerts through credit management agencies

9. At home, use spam blockers, firewalls, virus protection, and adware & malware destroyers

10. Update your Operating System whenever security patches are available

Please contact LSC Card Services for assistance. Our contact information is 1-800-304-2273 or email us at lscriskmgmt@lsc.net.