Daily Union Article
Saturday, August 13, 2016
Title: Online Data Breech & Identity Theft

In an August 8, 2016 consumer alert, Kansas Commissioner of Insurance, Ken Selzer shared that 240,115 Kansans who have insurance through Blue Cross Blue Shield (BCBS) of Kansas City should take measures to safeguard their financial and health information. A recent data breach allowed exposure of information from members' medical ID cards. Commissioner Selzer explains that an Explanation of Benefits summary sent to BCBS of Kansas City members can help them identify mysterious activity. For that reason, these reports should be reviewed carefully.

At this time, there is no indication that any of the stolen information from the BCBS of Kansas City breach is being used inappropriately, but the risk still remains. Although the data breach did NOT include Social Security numbers, dates of birth, banking or credit card information or medical claims, the press release serves as a reminder to all of us that we need to be diligent in our efforts to protect our personal information and identity. ***NOTE:*** This breach applied to BCBS of Kansas City members only. This is a separate company from Blue Cross Blue Shield of Kansas, Inc.

Your personal and financial identity is valuable. The possible ramifications when that information is stolen are far reaching. However, there are many things you can do to help prevent or reduce your exposure to identity theft.

One way to help reduce exposure is to limit the number of unwanted calls and emails you receive. While some phone calls and emails are important, others simply load up your inbox and others are simply illegal.

For example, if you don't want to receive prescreened offers of credit and insurance, you can opt out for a five year period or permanently. Making a toll-free phone call to 1-888-567-8688 will give you the avenue by which you can opt out of these offers for up to five years.

For a permanent block of these solicitations, you need to begin the process online at www.optoutprescreen.com and download the Permanent Opt-Out Election form, then sign and send it in. This service is operated by the major consumer reporting companies and they can put a stop to these unwanted solicitations.

Reduce your emails by discontinuing automatic notices, newsletters, and advertisements. Bookmark those sources so that YOU choose when contact is made, not the company.

Reduce exposure to identity theft by educating yourself about privacy rights. Federal law gives you the right to stop some sharing of personal financial information, but you have to advocate for yourself. If you are unsure what your rights are, you can ask the company or bank to provide you with their privacy practices and policy. You can then what is optional information and that which they are required by law to provide. The federal law balances your right to privacy with a company's need to provide information for normal business practices. The Federal Trade Commission (FTC) outlines your consumer rights in regards to information sharing. The FTC provides this guidance:

What your financial company CAN provide to non-affiliates without providing an opt-out:

- Information about you to firms that help promote and market the company's own products or products offered under a joint agreement between two financial companies
- Records of your transactions such as loan payments, credit card or debit card purchases, and checking and savings account statements to firms that provide data processing and mailing services for your company
- Information about you in response to a court order
- Your payment history on loans and credit cards to credit reporting companies

A privacy notice contains information about the company's data collection and information sharing practices. Reading these notices is important to knowing what is being shared about you and serves as the tool you can use to choose to opt-out. When you opt-out, you limit the amount of information the company can share about you. If you don't opt-out, then the company is free to share certain personal financial information. If you didn't initially take the opportunity to opt out, you can always change your mind and opt out of certain information sharing. For more information from the FTC, go to: https://www.consumer.ftc.gov/ and search for "privacy choices."

Reducing your exposure to personal and financial identity theft includes taking action with how you use technology in conducting personal business. Your computer is a valuable source to hackers that want to steal your information. When you are disposing of old computers, be careful that you clean the hard drives which may contain personal information. The computer owner's manual, the manufacturer's website, or its customer support service can provide you with information about how to clean the hard drive. If you use a software program designed for this purpose, consider using a program that overwrites or wipes the hard drive multiple times; otherwise, the deleted information could still be extracted by someone with the right skill set.

Unfortunately, we live in a world of fraud and scams, so it is important that you use trusted sources when you share information online. Do your homework to make sure the websites you purchase from are protected with rigorous security systems. Even those that have these systems in place are susceptible to a breach of data – the hackers work to break through those safeguards just as hard as the security systems do to build thick and encrypted walls of protection.

Awareness and being proactive can serve as your best tools against personal and financial identity theft. For more information about protecting yourself from personal and financial identity theft, call me at the Geary County K-State Research and Extension office at 238-4161. Until next time, keep living resourcefully!