Consumer Watch

A Monthly Newsletter from the Connecticut Department of Consumer Protection

William M. Rubenstein, Commissioner *Dannel P. Malloy, Governor*

www.ct.gov/dcp Vol. 4, No. 3 October 2014

In This Issue

Suggested Links

www.ct.gov/dcp
Our website offers the latest and most comprehensive information that we have on dozens of consumer-related topics!

www.smartconsumer.ct.gov
Basic information to protect yourself and avoid scams!

https:www.elicense.ct.gov
To verify a license, permit or registration, or to run a roster of licensees. Also, the place for online renewal!

Contact Us

www.ct.gov/dcp

dcp.communications@ct.gov

Find us on facebook

Health Care Identity Theft is On the Rise -- Are You Protected?

Last month we advised consumers yet again to change passwords and check their credit in the wake of another massive data breach, this time involving more than 56 million credit and debit cards used at Home Depot earlier this year. Hopefully, the frequency of these incidents is not leading to complacency among consumers, because a major wave of issues may be on the horizon as scammers aggressively turn their attention to the health care sector.

In late September, Reuters reported that medical information is "worth 10 times more than credit card number[s] on the black market," and that cyber- criminals are increasingly targeting the $3 trillion U.S. healthcare industry, in which many companies still rely on aging computer systems that lack updated security features.

The Identity Theft Resource Center reports that 2013 saw the health care industry experience more data breaches than ever before, accounting for 44% of all breaches and surpassing all other industries, including the financial services industry. To illustrate, last month Community Health Systems, a hospital chain with facilities in 29 states, was hacked and the names, addresses, birth dates and Social Security numbers of 4.5 million patients were stolen.

more, page 3

Identity theft continues to be a problem for everyone, as technologies evolve and highly-skilled hackers gain access to huge databases and sell information across the globe. This month we focus on the importance of safeguarding health care records and health insurance information, which, along with your social security number, are hot targets for thieves. Will freezing your credit reports make it simpler for you to protect your good name? Page 3 offers some of the pros and cons. We're looking forward to our first "Cross-Cultural Symposium" later this month, and probably like most who have registered, we're eager to start applying the strategies we learn; details on page 2. Our Gaming Division works tirelessly behind the scenes to ensure the integrity of all legal gaming in the state. You can read about their most recent success at thwarting criminal activity on page 4. Finally, in many households, the race is on for the perfect Halloween costume! Our sidebar on page 2 offers a few reminders that can prevent Halloween injuries. Wishing you all the best,

Bill Rubenstein

Suiting Up Safely for Halloween

Overseeing child and product safety is an important aspect of the Department of Consumer Protection's overarching mission, so Halloween is a perfect opportunity to offer these safety reminders.

- To assure maximum fire-safety, look for costumes made from 100% synthetic fibers like nylon or polyester with a "Flame Resistant" label.
- Although this label doesn't mean these items can't possibly catch fire, it does indicate the items will resist burning and should extinguish quickly once removed from the ignition source.
- Avoid glitter, which tends to be somewhat flammable. (It also has been known to contain lead.)
- Capes, trains, and dangling sleeves are doubly risky -- not only can they graze a flame-lit jack-o-lantern and catch fire, they also pose a tripping hazard.
- If making your own costumes, use polyester, nylon, wool, and acrylic fabrics -- avoid cotton balls, twine and other highly flammable natural fibers.
- Make sure costumes are not too loose-fitting and that shoes fit well.
- Finally, make sure masks don't obstruct vision; face makeup is a much safer option.

Waiting List Only: Tremendous Registration Response for State's First Cross-Cultural Communication Symposium

Everywhere one looks, the rapid influx and dramatic diversity of immigrants and refugees are changing the landscape of our cities, towns, neighborhoods and rural areas. How do we, as service providers charged with offering aid, education, and all manner of support and orientation to these diverse populations, meet the challenge? This question and many others will be considered and discussed in a series of lively panels on October 23rd, as the Department of Consumer Protection offers "Cross Cultural Communication: How to be Heard," a free- day-long event in Hartford.

Catherine Blinder, who since January of this year, is the Department's Chief Officer of Outreach and Education, has been the primary organizing force behind this groundbreaking event.

"To our knowledge, this is the first statewide symposium that addresses the opportunities and challenges facing those in Connecticut who provide services and assistance to diverse communities who make Connecticut their home," Ms. Blinder said. "The symposium will bring together the best and brightest minds in the country – challenging the assumptions and communication practices that exist, and offering science, experience, research and anecdotal information to inform a new way of thinking."

Symposium planners hope to videotape the program, which will include the following panels:

Know Your Audience? Moderated by: Susan Campbell
Panelists: Seth Hannah, MA Institute of Technology, Anthropology Program; Jennifer Leach, Community Ed. Specialist, Federal Trade Commission; Kien Lee, Vice-President, Community Science; Jann Murray-Garcia, University of Southern California, School of Medicine

Brokers, Intermediaries & Influencers Moderated by: Homa Naficy
Panelists: Janet Bauer, Trinity College, International Studie; Vikki Katz, Rutgers University School of Communication and Information; Rachel Peric, Deputy Director, Welcoming America; Abigail Williamson, Trinity College, Political Science

Ethnic Media: Front and Center Moderated by: John Dankosky
Panelists: Sandy Close, Executive Director, New America Media; Jehangir Khattak, Communications Director, City University Graduate School of Journalism's Center/ Center for Community Ethnic Media; Hussien Mohamed, Sagal Radio

The Power of Storytelling Moderated by: Kristina Newman-Scott
Panelists: Keiron Bone, Welcoming America; Lauren Burke, Executive Director, Atlas: DIY; Jack Doppelt, Northwestern University, Medill School of Journalism; Carmen Gonzalez, Rutgers University, School of Communication & Information

True or False?

If my favorite local restaurant runs out of their house wine while I'm having a party at their facility, they can send someone out to the store to buy more. ***True or False?*** **Answer, page 4**

Is a credit freeze a security option for you?

With frequent news reports of large-scale data breaches, consumers want to know whether it's worth opting to freeze their credit. There are pros and cons to this, depending on how often YOU may need a credit report.

A credit freeze lets you limit access to your credit report, which makes it more difficult for anyone -- including identity thieves -- to open new credit accounts in your name. Most creditors want to see your credit report before they approve a new account, and if they can't view your records, they often won't grant any new credit.

But a credit freeze won't stop an identity thief from charging to any existing accounts. So even if you "freeze" your credit, you still need to monitor your existing credit and bank accounts for charges you don't recognize.

The freeze remains in place until you ask the credit reporting company to temporarily lift it or remove it. A credit reporting company must lift a freeze no later than three business days after your request. Know that there are costs to initiate the freeze and to lift the freeze, which vary by state.

A credit freeze won't affect your credit score, nor will it prevent you from getting your free annual credit reports, opening a new account, applying for a job, buying insurance or renting an apartment, but it will require you to lift the freeze temporarily in order to do these things.

If you choose to place a credit freeze on your credit reports, contact each of the nationwide credit reporting companies:

- Equifax — 1-800-525-6285
- Experian —1-888-397-3742
- TransUnion — 1-800-680-7289

You'll need to supply your name, address, date of birth, Social Security number and other personal information along with a fee, ranging from about $5 to $10. Each company will then send you a confirmation letter containing a unique PIN or password; keep this safe. You'll need it when you want to lift the freeze.

To be sure your existing accounts aren't being misused, regularly check your credit reports and statements, which costs you nothing. If you want the added security of knowing that no new accounts can be opened, a credit freeze can be a useful supplement.

NEXT MONTH: ABOUT CREDIT ALERTS

Health Care Identity Theft, continued from page 1

What this means to you

Theft of medical record information can affect you in a number of ways. A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If a thief's health information is mixed with yours, your own medical treatment, insurance and payment records, and credit report could be affected.

What to watch for

To spot possible health care fraud, always read your medical and insurance statements thoroughly, including your Explanation of Benefits statements or Medicare Summary Notices; they will show warning signs. Look at the name of the provider, the date of service, and the service provided. Do the claims paid match the care you received? If you see a mistake, contact your health plan and report the problem.

Other warning signs:

- a bill for medical services you didn't receive
- a call from a debt collector about a medical debt you don't owe
- medical collection notices on your credit report that you don't recognize
- a notice from your health plan saying you reached your benefit limit
- a denial of insurance because your medical records show a condition you don't have

You can help prevent health care fraud

1. Guard your Social Security number. In medical records as well as financial records, your SSN is key. Most health care providers routinely ask for a social security number, but often don't need it in order to treat you. The SSN is primarily a tool for collecting overdue payments when necessary. If asked for your Social Security number, ask if the office will accept another means of identification.
2. Keep paper and electronic copies of your medical and health insurance records in a secure place.
3. Shred mail and documents that include personal information, such as hospital statements, outdated health insurance forms, or medical records that you no longer need. Don't just put these in the trash. Remove identifying information on prescription labels before you throw out empty canisters.
4. Never give medical insurance information or any other personal information to anyone over the phone or online unless **you** initiated the contact or you're absolutely sure that they are legitimate. Be wary if someone offers you "free" health services or products, but requires you to provide your health plan ID number. Thieves are known to pose as employees of insurance companies, hospitals, clinics, doctors' offices, and pharmacies to try to trick people into revealing sensitive information.

Continued, page 4

WTIC News Talk 1080 — AARP Real Possibilities in Connecticut

WTIC Shred Day

Sponsored by AARP Fraud Watch Network

Saturday, October 18

At EnviroShred

Free shredding - open to the public in East Hartford! (Limit of 3 boxes/bags per person.) EnviroShred is a social enterprise of Easter Seals Capital Region & Eastern Connecticut. The AARP Fraud Watch Network is fighting identity theft and fraud. Saturday, October 18th, from 10 am until 2 pm at EnviroShred, 22 Prestige Park Circle in East Hartford. All are welcome. www.wtic.com/shredday

Quick Action Leads to Identification and Recovery of Convicted Lottery Ticket Scammer

Upon fielding several complaints from consumers in Bridgeport and Norwalk during the last week of September, the Department's Gaming investigators were concerned that someone was selling scratched-off instant lottery tickets that they claimed were winning tickets, when in fact they were worthless. Victims reported buying these alleged winning tickets for between $500 and $2,000 after being told that they could cash them in for the winning prize of $20,000, -- only to find out they were fake.

The Department obtained surveillance photographs of a person of interest involved in the scam, and on Friday September 26th, issued a warning to consumers. The agency included a photo of the possible suspect and asked for the public's help in identifying him.

Within a day, an investigator from New York State Lottery contacted our investigators with information that the suspect had recently been paroled after serving time for similar crimes in that state. New York and Connecticut officials collaborated to locate the individual two days later in Delaware, where he will be served with an arrest warrant from Connecticut and then arrested for violating the terms of his New York State parole.

"This is a fine example of interagency collaboration," Commissioner William M. Rubenstein said. "We're grateful to New York for being so quick to reach out and help us to identify this person, stop his scam, and bring our investigation to a close."

Consumers are reminded to buy lottery tickets only from authorized lottery retailers. Red alarm signals should go off anytime someone is trying to sell a so-called "winning" lottery ticket. Scammers typically will list a variety of reasons why they cannot cash in the ticket themselves. Then they will offer to sell the "winning" ticket for a sizeable amount, but an amount still substantially less than the value of the "prize-winning" ticket. Of course, there will be a sense of urgency to complete the transaction, leaving the victim little time to think or validate the truth of the story.

The only correct way to verify a winning ticket is through a retailer's lottery terminal or on the Lottery Ticket Checker available in all Lottery Retailer locations. Don't take the word of anyone who offers you a "winning ticket" for cash. If approached by someone offering to sell you a winning lottery ticket, just decline, leave the immediate area, and contact local law enforcement or the Department of Consumer Protection to provide a description of the con artist and any information that can assist authorities in stopping the scam.

True or False? Answer
(from page 2)

The answer is **False**.

All alcohol must be purchased from a wholesaler. A permitted establishment that buys wine, beer or other alcoholic products from a package store for retail use risks a fine and/or suspension of its liquor permit.

Health Care Identity Theft, continued from page 3

5. Finally, don't get hooked by a "phishing" scheme. Delete email or text messages that ask you to confirm or provide personal information. The sender may even try to prove they are legitimate by including some personal information about you in their message. Chances are this information was stolen as part of a data breach. Don't give them anything else! Legitimate companies don't ask for sensitive personal data via email or text.

What to do if you suspect fraud

If you suspect a thief used your medical information, follow these steps from the Federal Trade Commission.