Robinson+Cole

Data Privacy + Cybersecurity Insider
Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Ransomware Attack Hits Dallas Senior Living Community

No industry is immune from ransomware attacks—including senior living communities. Senior living communities have exploded now that baby boomers are selling homes, downsizing, and getting ready for that stage of life. Many of us in the sandwich generation are choosing communities for our parents. When residents move into a senior resident community, the community collects a vast amount of personal information from the resident. This information is valuable to hackers, and if security measures to protect the information are not robust, a hacker can gain access to this information and commit fraud against one of our most vulnerable populations—our seniors. *Read more*

WannaCry Also Encrypted Hospital Medical Devices

The fallout from WannaCry continues, particularly in the health care sector. There are new reports that WannaCry affected at least two hospital systems in the U.S. and encrypted medical devices (power injector systems) in the hospitals. There are additional anecdotal reports that other medical devices were affected by WannaCry. *Read more*

HHS Office of the Assistant Secretary for Preparedness and Response Issues Series of Cybersecurity Updates in Response to WannaCry Attack

In response to the WannaCry ransomware attack that infiltrated the computer systems of health care systems and other entities worldwide on or around May 12, 2017, (previously discussed here), HHS's Office of the Assistant Secretary for Preparedness and Response (ASPR) issued a series of updates to provide consumers and potentially affected organizations with information on the attack and to detail HHS's efforts to mitigate the harmful effects of the attack on government computer systems and health care organizations. *Read more*

May 25, 2017

FEATURED AUTHORS:

Conor O. Duffy
Linn Foster Freedman
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Enforcement + Litigation
Data Breach
Drones
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

DATA BREACH

Rite Aid's Online Store Breached

Rite Aid has admitted that its online eCommerce platform was accessed an unauthorized individual(s) from January 30, 2017, through April 11, 2017, and its customers' names, addresses, and payment card information, including credit and debit card numbers, expiration dates, and security codes were compromised. The breach affected any customers who used Rite Aid's online store and entered their payment card information during those dates. Rite Aid is offering affected individuals 12 months of identity theft monitoring. *Read more*

ENFORCEMENT + LITIGATION

Target Settles with 47 AGs and DC for $18.5 Million

The 2013 hack that caused one of the largest breaches in U.S. retail history continues to be a headache for Target Corp. Following the breach just before the holidays in 2013, Target was hit with consumer class action suits, suits by credit card companies, hostile shareholders at its shareholders' meeting, and investigations by 47 state attorneys general and the District of Columbia (DC). Target has announced that it has reached a settlement to end the investigation of the 47 state AGs and DC for $18.5 million—the largest data breach settlement with multiple AGs in history. *Read more*

Kmart Breach Settlement of $6.9 Million with Banks Approved by Court

Kmart's proposed settlement with banks that required it to reimburse customers following its 2014 data breach was approved by an Illinois federal judge last week with one caveat: he wants to see how much each bank is being paid from the settlement, and he wants to see the billings records of the plaintiffs' attorneys. The proposed deal reimburses the banks with a payment of $5.2 million and pays the lawyers $1.7 million in attorneys' fees. *Read more*

Protection of Vendor Report and Documents as Work Product Is Big Win for Experian

When assisting clients with an emergency data breach response and preparing and implementing a data privacy and security plan, it often becomes efficient, cost-effective, and necessary to hire outside

vendors to assist with portions of the engagement. These activities include risk assessments, gap assessments, vulnerability testing, forensic analysis, and security incident investigations. *Read more*

Gather App Hit with TCPA Class Action Suit

Gather, a free app designed to allow users to create event invitations and send them to their contacts, has been hit with a proposed TCPA class action suit. The named plaintiff alleges that Gather tricks users into giving it their contacts and then uses the contact information to send unsolicited texts to their contacts without express written consent, a violation of the Telephone Consumer Protection Act. The complaint further alleges that Gather intentionally misleads users when asking for access to their contact information. *Read more*

DRONES

The Drone Economy in the Construction Industry

Drone data is used in construction (3-D mapping, site surveying), agriculture (crop mapping), energy (solar and wind turbine monitoring), insurance (roof inspections), infrastructure (inspection), communications (damage assessments) and countless other industries. These industries, and more, have long sought data "from above," generally from satellites or airplanes, but drones are better sensors in the sky. Drone can gather higher-resolution images and more frequent data than satellites, and they are cheaper, easier to use, and safer than airplanes. Drones can also provide "anytime, anywhere" access to views with accuracy that rivals laser scanning—and the technology has not even reached its peak. *Read more*

FAA Drone Registration Rule Doesn't Apply to Model Aircraft

The D.C. Circuit ruled late last week that the Federal Aviation Administration (FAA) Drone Registration Rule does not apply to model aircraft. The court held that the FAA does not have authority to regulate model aircraft under the FAA Modernization and Reform Act of 2012 and, therefore, vacated the drone registration rule for model aircraft. *Read more*

Amazon's Air Traffic Control System for Package Delivery Drones

Amazon announced this week that its development of an air traffic control system for its package delivery drones (and other commercial drones flying in the national airspace) has taken off—pun intended.

This air traffic control system would support Amazon's package delivery system from the warehouse to the customer's doorstep. It was created by a research and development team in Paris, France, to ensure that delivery drones don't collide with buildings, trees, birds, or other drones. Amazon hired engineers with expertise in aviation as well as machine learning and artificial intelligence. *Read more*

PRIVACY TIP #89

10 Tips to Help Protect Senior Loved Ones' Privacy

It is hard enough for middle agers like me to keep up with all the ways our personal information can be collected, accessed, used, disclosed, sold, or stolen. It is even harder for our loved ones who are older, but not necessarily wiser in the digital age.

Here are some tips for caregivers to keep a handle on their senior loved ones' privacy and help them avoid becoming victims of frauds and scams:

1. Put their home and cell phone numbers on the do-not-call list.
2. Check their bank statements to review any direct withdrawals to determine whether they are legitimate. Stop all withdrawals that are not necessary, out-of-date, or inapplicable to their living situation. Encourage them to stop giving their bank account information to anyone.
3. Educate them about giving their personal information to others, including their senior living community. Just because there is a box or line on a form does not mean that it should be filled in. For instance, the assisted living facility does not need the senior's driver's license number. Don't give them (or anyone else) any information that they do not have a need to know or have.
4. Counsel your senior loved one about scams perpetrated over the phone and not giving any of their personal information over the telephone. Let them know the IRS never calls people on the phone for back taxes.
5. Monitor and assist them with their social media activity.
6. Advise them not to keep personal information out in the open for others to view or steal.
7. Advise them not to keep their Social Security card or Medicare card in their wallet or purse or in the top drawer of their desk.
8. Help them with their privacy settings on their smartphone and explain what they mean and do.
9. Encourage them to ask for your help if they need it or don't understand something. Technology can be intimidating, and they need to feel comfortable in asking questions.
10. Vet and monitor caregivers carefully.

Frauds are getting more and more sophisticated, and schemes are targeting seniors. Give your loved ones the information they need to

protect themselves from becoming victims.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

Robinson & Cole LLP