Attorney Advertising

September 10, 2015

Data Privacy + Security Insider

DATA BREACH

10 Million Excellus Blue Cross Blue Shield Members' Information Compromised

Yesterday, Excellus Blue Cross Blue Shield, located in Rochester, NY, announced that it will notify up to 10 million members that it was the victim of a cyber attack dating back to December of 2013 that exposed their members' names, addresses, and Social Security numbers, telephone numbers, member identification numbers, financial account information and claims information.

The breach was detected on August 5. The insurer is notifying the affected individuals and will offer identity theft protection services.

This breach is in the wake of the Anthem breach which affected 80 million individuals. Many have predicted that health insurers would be targets of sophisticated hackers and these incidents are proving those predictions to be correct.

— Linn Foster Freedman

UCLA Suffers Another Data Breach

Last week, UCLA notified 1,242 patients that their health information may have been compromised in July when a faculty member's laptop was stolen.

UCLA has notified the patients, the Office for Civil Rights and the California AG of the data breach.

Tough going for UCLA, which also suffered a cyber attack on its information systems in July exposing over 4.5 million patient records (view related post).

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

UCLA Cleared in Lawsuit Alleging Breach as to Sexually Transmitted Disease Information

UCLA was absolved by a California judge last week in a suit filed by a patient of a UCLA affiliated doctor's group, who alleged that a temporary worker in the doctor's office used the doctor's username and password to get into her boyfriend's previous girlfriend's medical record. The medical record contained information that the previous girlfriend had a sexually transmitted disease.

The temporary worker texted photos of the medical records to her boyfriend and others.

The previous girlfriend alleged $1.25 million in damages as a result of the unauthorized disclosure. UCLA defended the action stating it could not be held responsible for misconduct of an affiliated doctor's temporary employee.

The judge agreed and dismissed the complaint.

This result is quite different than the very similar fact scenario against Walgreen Company when a pharmacist accessed and disclosed sexually transmitted information of a former girlfriend to her boyfriend. Walgreens was tagged by a jury for $1.4 million in that case, despite the fact that the pharmacist admitted she was outside the scope of her employment and violated Walgreen's policies when she accessed and disclosed the information. The decision was upheld by the Court of Appeals of Indiana.

— Linn Foster Freedman

Does Facebook's Collection of Photos Violate Privacy Laws?

An Illinois man recently filed a proposed federal class action alleging that Facebook violates state law protecting the privacy of biometric data through its alleged collection of facial recognition data from over a billion faces on uploaded photos.

As many Facebook users are aware, the social networking service automatically matches persons in uploaded photos. According to the lawsuit, this is done by scanning geometric data from faces after users "tag" (provide the name) a person in a photo not known to Facebook.

The named plaintiff in the suit, Frederick Gullen, is not a Facebook user and alleges that he never consented to Facebook allegedly acquiring his facial features taken from a photograph uploaded by another person. He seeks to represent a class of Illinois residents who are non-Facebook users but have been tagged in photos on Facebook.

The Illinois Biometric Information Privacy Act regulates capturing, using and transferring facial scans and other data "as biometric identifiers." The state statute also covers "biometric information," which it defines "as any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual..."

Illinois law prohibits companies that collect biometric data from selling it to third parties. During a 2012 U.S. Senate hearing, Facebook refused to commit that such information would not be sold.

Facebook has stated publicly that it considers the suit to be meritless and that it intends to defend itself

vigorously. While Facebook has yet to formally respond to the complaint, one of the arguments it will likely make is that the statute at issue excludes information derived from photographs.

The case is *Gullen v. Facebook Inc.*, case number 1:15-cv-07681 in the U.S. District Court for the Northern District of Illinois.

— Brian J. Wheelin

DATA SECURITY

Interim Rule Requires Department of Defense Contractors to Report Cyber Breaches

Companies doing business with the U.S. Department of Defense are facing new requirements for reporting data security breaches and for acquiring cloud computing services. The Interim Rule, effective August 26, 2015, amends the Defense Federal Acquisition Regulation Supplement (DFARS) to implement sections of the National Defense Authorization Act for Fiscal Years 2013 and 2015, which require DoD contractors to report network penetrations resulting in a compromise of covered information within 72 hours. The type of information covered by the Interim Rule includes controlled technical information, export controlled information, critical information and other information requiring protection by law or regulation. The Interim Rule also establishes new policies for contracts covering cloud computing, including the requirement to maintain government data within the United States. Given the urgency of implementing federal cybersecurity measures protecting sensitive defense information, the Interim Rule went into effect immediately, with comments due October 26, 2015 to be considered in the final rule. The Interim Rule is available for review here.

— Benjamin C. Jensen

National Futures Association Proposes Cybersecurity Rules for its Members

The National Futures Association (NFA) recently approved new mandatory cybersecurity rules for members of the futures industry. Members of the NFA include exchange-traded futures, forex and over-the-counter swaps industries. The rules are in response to recent data security breaches.

The rules require members to implement an information security program, including a security and risk analysis, outline of the safeguards put in place, and security incident detection, investigation and mitigation. The programs also require members to train personnel on data privacy and security and continually evaluate the security program.

— Linn Foster Freedman

Approximately 8,000 Fiat Chryslers Recalled for Hacking Vulnerabilities

If you drive a Fiat Chrysler sport utility vehicle (SUV), you may want to check to see if your vehicle is one of the almost 8,000 vehicles recalled this week after discovery of a software flaw that may expose the vehicle to security vulnerabilities and potentially allow easy access for hackers to the vehicle's software systems. Fiat Chrysler reported that the recall involves 7,810 2015 Jeep Renegade SUVs with touchscreens. We had previously reported the recall of over 1.4 million Dodge, Ram, and Jeep vehicles

back in July due to the same software hacking vulnerabilities.

All those Fiat Chrysler drivers affected by this recall will receive a USB that can be used to update the software and provide additional security features to better protect the vehicle from hackers. Fiat Chrysler said, “No defect has been found,” but it “is conducting this campaign out of an abundance of caution.” The company also said that “the software manipulation addressed by this recall required unique and extensive technical knowledge, prolonged physical access to a subject vehicle and extended periods of time to write code.” Surely, this recall exemplifies some of the security concerns we may have as the internet of things continues to grow.

— Kathryn M. Rattigan

HEALTH INFORMATION

NLRB Extends its Email Rule to the Health Care Workplace

The National Labor Relations Board (Board) continues its scrutiny of employer policies—this time striking down an email policy designed to ensure that health care employees provide patient care without distraction. UPMC, 362 NLRB No. 191 (August 27, 2015). To read the full story, click here.

— Natale V. Di Natale

DATA PRIVACY

U.S. Department of Education Issues FERPA Guidance Related to Medical Information

In conjunction with the new school year, the U.S. Department of Education issued guidance, in the form of a "Dear Colleague" letter, to higher education institutions to remind them of FERPA's requirements as they relate to the provision of medical and mental health services to students in higher education institutions.

The letter outlines the protections afforded to student medical records when litigation occurs between the institution and the student. In particular, institutions should not share student medical records with the institution's attorneys or courts "unless the litigation in question relates directly to the medical treatment itself or the payment for that treatment, and even then disclose only those records that are relevant and necessary to the litigation."

The letter further outlines the exceptions under which student medical records may be disclosed without consent of the student under FERPA. They include:

- To school officials, including professors, administrators, and legal counsel, provided the institution has determined that those officials have a legitimate educational interest in the records. The exception only allows school officials with the function and responsibility to view only the records that are necessary to fulfill a professional responsibility.

- Campus counselors and mental health professionals may disclose student health records to campus threat assessment teams about a threat to a student's safety or the safety of others to prevent or respond to violence on campus.

- Attorneys representing institutions in legal proceedings if the medical treatment or payment for that treatment relates directly to the litigation, and only then, the minimum amount necessary. Otherwise, the records should not be disclosed without consent or a court order.

- In response to a subpoena or court order, but the disclosures should be limited to only those records that are relevant and necessary to the litigation.

- To appropriate parties if the student "poses an articulable and significant threat to self or the health or safety of other individuals, including law enforcement, public health officials, trained medical personnel, and parents." The information disclosed should only be those necessary to protect the student or others.

— Linn Foster Freedman

CYBERSECURITY

32 Alleged IRS Hackers Arrested

The federal government has arrested 32 members of the Insane Crip gang and charged them with 283 counts of criminal conspiracy, 299 counts of identity theft, 226 counts of grand theft and 58 counts of attempted theft through a $14.3 million identity theft and tax fraud scheme of filing fraudulent tax returns.

Millions of Americans have been victims of tax return fraud, and although this is a small solace, it's a solace nonetheless.

— Linn Foster Freedman

European Authorities Arrest Alleged Banking Malware Developers

Law enforcement authorities have announced the arrest of two individuals—one a Russian national and the other Moldovan, both of whom are alleged to have developed and implemented banking malware known as Citadel and Dridex. The sophisticated malware are reported to have been used to steal millions of dollars from U.S. financial institutions. They are awaiting extradition to the United States.

— Linn Foster Freedman

For more thoughtful and timely discussions of legal news and perspectives on issues relating to data privacy and security, subscribe to our *Data Privacy + Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.

© 2015 Robinson & Cole LLP. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission. This document should not be considered legal advice and does not create an attorney-client relationship between Robinson+Cole and you. Consult your attorney before acting on anything contained herein. The views expressed herein are those of the authors and not necessarily those of Robinson+Cole or any other individual attorney of Robinson+Cole. The contents of this communication may contain attorney advertising under the laws of various states. Prior results do not guarantee a similar outcome.