Attorney Advertising

Robinson+Cole

Data Privacy and Security Insider

May 28, 2015

DATA BREACH

With the IRS Breach, It's Clear Your Data is at Risk

The Internal Revenue Service (IRS) released on Tuesday, May 26, 2015, news of a major data breach estimated to have affected 100,000 U.S. households' tax returns. The data was wrongfully obtained from an IRS application known as "Get Transcript," which allows taxpayers to access their prior tax returns. This data includes Social Security numbers, dates of birth, and street addresses of individuals who have filed tax returns. The hackers used the data to produce a fake 2014 tax return, and then requested that the IRS send a tax refund to a hard-to-trace debit card.

Although only a small percentage of American households have been affected, the impact is significant. The IRS stated that since the hackers were already in possession of personal information belonging to the affected taxpayers, the hackers were able to clear the multi-layer authentication process, which asks the applicant a series of personal questions with the expectation that only the taxpayer could provide correct details.

Where might a hacker easily access a taxpayer's personal information? How about social networks such as Facebook, Instagram, or LinkedIn? Social networks often encourage members to complete their public profile by answering questions such as:

1. Who was your high school mascot?
2. What city were you born in?
3. What is your favorite sports team?

The social networks presumably want to connect similar individuals—perhaps old friends or schoolmates. On the other hand, hackers can access this personal information as well, especially if your profile is public. Even if your profile is set to a private security setting, hackers may be able to find a way to access this information. It's best to assume that any information shared on a social media network can be viewed by anyone, and potentially used by them for other purposes.

Look for the Obama administration to increase the IRS budget in 2016 in an effort to enhance its data security infrastructure to protect taxpayer data. We expect further developments in the coming weeks and will keep you updated on any progress.

– James Merrifield and Linn Foster Freedman

Adult FriendFinder Confirms Data Breach of its Users' Personal Information

On May 22, 2015, an online dating service called Adult FriendFinder confirmed that there had been a data breach of ***some*** of its 64 million users' personal information. In an online notice to its users, Adult FriendFinder said that it only recently became aware of this cybersecurity breach, and that it was working closely with Mandiant, a third-party cyberforensics expert, and law enforcement officials, including the FBI, to uncover the source of the breach. Adult FriendFinder also disabled username search functions and masked usernames of all members it believes may have been affected by the breach. A company representative said, "This means that our members will still be able to log-in using their username and password but the search function will be disabled in an effort to protect member privacy. We are also in the process of communicating directly to members on how to update their usernames and passwords."

At this point Adult FriendFinder claims that no financial information or user passwords have been compromised, but they have yet to release any information on the specific types of information they do believe may have been accessed by hackers. A company representative said, "As is common with similar cyberattack events, until the investigation is completed, it will be difficult to confirm the full scope of the incident, but we will continue to work vigilantly to address the potential issue and will provide updates on this site as we learn more from our investigation."

However, it has been speculated by some United Kingdom news sources that over 4 million Adult FriendFinder members information, including sexual preferences, sexual histories, e-mail addresses, usernames, dates of birth, postal zip codes, and unique Internet protocol addresses, have been stolen and leaked on 'dark' websites. We will update you on the specifics of this breach once Adult FriendFinder releases additional information as the investigation progresses.

– Kathryn M. Sylvia

FTC Says Self-Reporting is Likely to Result in More Favorable Resolution

Last week, the FTC encouraged companies to self-report data breaches with the promise of more likely favorable treatment. The statement comes in a blog post, authored by Mark Eichorn, an Assistant Director in the FTC Bureau of Consumer Protection's Division of Privacy and Identity Protection. Although the post provides a general overview of an FTC investigation of a potential data breach, its ultimate point is that it is better to disclose a problem yourself than wait for the government to come knocking.

Self-reporting is a hotly debated concept right now, not because it is novel, but because dealings with the government over the last several years have called into question whether there are, in fact, any benefits to disclosing a problem to federal or state authorities. This is true in all regulatory spheres, not just data privacy and security.

In a typical scenario, after a company discovers a data breach or other problem, it promptly conducts an independent, thorough and complete investigation. The investigation findings are used to institute remedies and safeguards to avoid a similar problem in the future. Next, company leadership, in conjunction with counsel, determines whether to tell the government about the problem or stay quiet, hoping the government never comes knocking.

Self-reporting should be an easy decision: ideally, the government expresses appreciation for the company's candor, reviews and approves the remedial measures, and sends the company on its way. But that's not always the case. The government may initiate its own investigation, issuing demands for documents and witness testimony. The remedies and safeguards may be deemed inadequate. Fines and

penalties may be sought.

The worst case scenario should always be considered, but in this latest blog post the FTC seems to be offering self-reporters some assurances that it will work to avoid an unduly harsh result.

– Edward J. Heath

Nevada and North Dakota Amend State Breach Notification Laws

Nevada has amended its breach notification law, effective July 1, 2015, to include a medical or health insurance identification number and a user name, unique identifier, or e-mail address in combination with a password or code that allows access to an online account within the definition of personal information that requires notification if it is breached.

Similarly, North Dakota has amended its breach notification law to require any personal or entity—not just businesses in North Dakota—to notify North Dakota residents of a security breach involving their personal information. The amendment also requires notification of the breach to the North Dakota Attorney General's office if the breach affects more than 250 individuals. Finally, the amendment only requires notification if there is a breach of employee identification numbers if they are in combination with a security code, access code, or password that could be used to access the identification number. The North Dakota law becomes effective on August 1, 2015.

– Linn Foster Freedman

ENFORCEMENT + LITIGATION

FINRA Settles Data Breach Enforcement Action

The Financial Industry Regulatory Authority (FINRA) agreed to settle its enforcement action with Sterne Agee & Leach, Inc. (Sterne) this week for $225,000. The enforcement action followed the loss of an unencrypted laptop by an information technology employee when it was left in a restroom and was never recovered. The laptop contained the names, addresses, account numbers, and tax ID numbers of all account holders—approximately 350,000 individuals—that the firm had opened between 1992 and 2013.

In assessing the settlement, FINRA stated that Sterne failed to take appropriate precautions to protect the information and failed to have written security protocols to ensure that the information was safeguarded by appropriate technology.

FINRA has exercised regulatory authority over the security practices of financial entities under its jurisdiction, and has become more active in assessing fines and penalties. Businesses servicing the financial industry may wish to review existing security practices to determine whether they are using best practices in securing customer information, including encryption for mobile technology and laptops.

– Linn Foster Freedman

DATA PRIVACY

New Jersey Passes Motor Vehicle Data Privacy Law

We have commented before that many consumers do not know or understand the amount of data their motor vehicle has concerning their driving habits, including erratic driving, speed, whether the radio or Bluetooth is being used and when the brakes are used. This data can be used in numerous ways that were never contemplated before.

In response to concerns over the use of motor vehicle data, New Jersey Governor recently signed into law a bill aimed at limiting the access to, and use of, data recorded, stored, or transmitted from an automobile recording device. The law requires that the owner of the motor vehicle consent **in writing** to the "duration and scope of data retrieval, retention, and use, prior to or at the time the data is retrieved, obtained, or used."

Written consent is not required in certain circumstances, such as by law enforcement pursuant to a search warrant; it is used for "improving motor vehicle safety, security, performance, operation, compliance with traffic laws or traffic management…"; it is retrieved or obtained by a dealer and used for "the sole purpose of diagnosing, servicing, or repairing the motor vehicle"; it is accessed by emergency response personnel; or through a "legally proper discovery request or order in a civil action." This means that the data can continue to be requested in lawsuits involving motor vehicle accidents.

The law further prohibits the alteration or deletion of data within two years after a crash resulting in bodily injury or death.

Violation of the law carries the penalty of $5,000 for each offense payable to the New Jersey Motor Vehicle Commission.

– Linn Foster Freedman

MERGERS & ACQUISITIONS

LinkedIn Acquires Lynda.com for $1.5 Billion

LinkedIn has announced that it will acquire Lynda.com, a subscription online education service that offers hundreds of thousands of educational videos and over 6,000 online courses to its customers. LinkedIn stated that the purchase will expand LinkedIn's ability to offer professional development services to its members.

– Linn Foster Freedman

To get more thoughtful and timely discussions of legal news and perspectives on various issues relating to data privacy and security, subscribe to our *Data Privacy and 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 and Security Team.

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

---