NOW + NEXT

NP PRIVACY PARTNER | NIXON PEABODY LLP

March 1, 2019

What's trending on NP Privacy Partner

The FTC warns online romance scams are on the rise, the final OCR settlement of 2018 nets $3 million penalty and more. Here's what's trending in data privacy and cybersecurity.

Cybersecurity

FTC warns of proliferation of romance scams

The Federal Trade Commission (FTC) warns that online romance scams are increasingly leaving persons looking for love in all the wrong places. During 2018, the FTC's Consumer Sentinel Network received more than 21,000 reports of romance scams with aggregate losses totaling $143 million, which is more than any other consumer fraud type identified by Sentinel. The trend is a steady increase in such scams, which totaled 8,500 reports in 2015 with losses of $33 million.

The romance scammers create phony online profiles, often by lifting pictures off the web to make themselves appealing. They use fake names or assume the identities of real people. The scammers' reach is wide-ranging on dating apps as well as social media sites that are not generally used for dating (e.g., Facebook messaging). The scammers may also convey stories of blight and despair, such as the need for money due to a medical emergency. Or, they may portray themselves honorably as being stationed overseas.

The median individual loss to a romance scam reported in 2018 was $2,600, about seven times higher than the median loss across all other fraud types. The financial traps are plentiful through wire transfers or sending money using gift and reload cards.

Age apparently does not make people wiser to romance scams. Persons between the ages of 40 to 69 reported the highest losses to romance scams—more than twice the rate of millennials. Unfortunately, seniors over 70 reported the highest individual median losses at $10,000.

Common sense is vital when thinking that love may be in the air on the web. The FTC warns to never send money or gifts to any stranger, even one with the most convincing story of being a potential suitor or sweetheart. If the profile pictures seem too good to be true, try a reverse-image search of the pictures. If they're associated with another name or with details that don't match, you've uncovered a scam. Information is also available at ftc.gov/imposters. Persons targeted by or falling prey to a romance scam should report the activity to the dating or social media site, as well as the FTC at FTC.gov/complaint. –*Steven M. Richard*

Health Care & HIPAA

Final OCR settlement of 2018 nets $3 million penalty

On February 7, 2019, the Department of Health and Human Services, Office for Civil Rights (OCR) released information about its settlement with Cottage Health, a California hospital system. Following two breach reports from Cottage Health, OCR conducted an investigation that concluded with a resolution agreement and a settlement for $3 million.

The first breach resulted from a Cottage Health contractor's removal of electronic security protections from one of the system's servers. This caused protected health information (PHI) of approximately 50,917 individuals to be available to anyone with access to Cottage Health's server. The second breach, affecting 11,608 individuals, resulted from an employee misconfiguring a server, leading to PHI — including Social Security numbers — being accessible on the internet.

In its investigation, OCR determined that Cottage Health did not conduct a thorough and accurate risk assessment and failed to implement a risk management plan. In addition, highlighting that these security risk assessments are "living" documents, OCR found that Cottage Health did not periodically evaluate its technical and non-technical processes after environmental or operating changes that affected the security of its electronic PHI.

These breaches highlight two areas of compliance weakness for HIPAA covered entities and business associates: personnel and vendors. While there may not be a way to completely mitigate all risk that comes from the involvement of human actors and third-party vendors, an entity can take a number of steps to lessen its risk.

With respect to vendors, first and foremost, an entity must ensure that it has a HIPAA business associate agreement in place if PHI will be accessed, created or transmitted as part of the arrangement; OCR found that Cottage Health did not have a written business associate agreement with its contractor. A covered entity or business associate also should perform reasonable diligence of its potential vendors to ensure that they understand their privacy and security obligations and maintain robust HIPAA compliance programs.

Covered entities and business associates also are required to ensure that their workforces are trained in HIPAA compliance. In addition to education about regulatory requirements, an entity should train its personnel in the nuances of its compliance program specific to the services that it provides, the systems and processes that it employs, and the types of data that are relevant to an individual's job duties.

As part of its release about the Cottage Health enforcement action, OCR tallied its 2018 settlements and cases from HIPAA enforcement actions, which totaled $28.7 million.

The OCR press release can be found here and the resolution agreement can be found here. – *Valerie Breslin Montague*

Consumer Privacy

Proposed amendment would strengthen the power of the California Consumer Privacy Act

On February 25, 2019, the California Attorney General Xavier Becerra and Senator Hannah-Beth Jackson introduced proposed amendments (SB 561) to the California Consumer Privacy Act (CCPA), which was enacted in June 2018.

We previously discussed the breadth and novelty of the CCPA. SB 561 proposes to expand and strengthen the CCPA. Specifically, SB 561 would:

- Expand the consumer's right to bring a private cause of action if their rights under the CCPA are violated. As written currently, the CCPA only gives a consumer a private right of action if their non-encrypted or non-redacted personal information is subject to "unauthorized access and exfiltration, theft[] or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures...."

- Remove language allowing businesses 30 days to cure an alleged violation of non-compliance.

- Remove language permitting a business or other third party to seek the opinion of the attorney general for guidance on how to comply with the CCPA. Rather, the proposed amendment specifies that the attorney general may publish materials that provide general guidance on compliance.

If enacted, this would be the second amendment to the CCPA, which is set to become effective on January 1, 2020. – *Jenny L. Holmes*

For more information, please contact:

— Steven M. Richard at **srichard@nixonpeabody.com** or 401-454-1020
— Valerie Breslin Montague at **vbmontague@nixonpeabody.com** or 312-977-4485
— Jenny L. Holmes at **jholmes@nixonpeabody.com** or 585-263-1494

NP PRIVACY PARTNER BLOG

Staying ahead in a data-driven world: insights from our Data Privacy & Security team