

# University Cyber Roundup: Disruptions, Data Breaches, Financial Loss

Jan – Jun 2017

## Disruptions

**Los Angeles Valley College** was the victim of ransomware that shut down its website and e-mail system until a **\$28,000 ransom** was paid.

Los Angeles Valley College, CA / Jun 2017 / [Story](#)

## Data Breaches

Approximately **25,000 students, staff, and faculty members** from the University of Alaska had their personal information stolen, **including names and Social Security numbers**, following a successful phishing scam and subsequent data breach.

University of Alaska, AK / Jun 2017 / [Story](#)

**Oklahoma University exposed tens of thousands of students' data** including **social security numbers, financial aid information and grades** dating to at least 2002 due to lax security measures.

Oklahoma University, OK / Jun 2017 / [Story](#)

A **locked safe containing a hard drive with PII** on it **was stolen** from Washington State University in April.

Washington State University, WA / Apr 2017 / [Story](#)

**Names and e-mail addresses of individuals were compromised** when a University of South Florida employee sent out a mass e-mail without blind carbon copying individual's names. A **complaint was filed with the department of Health & Human Service, Office for Civil Rights** by one of the recipients.

University of South Florida, FL / Apr 2017 / [Story](#)

A Washington University School of Medicine **employee fell for a phishing email** designed to look like an official request for information, **releasing names, birth dates, and Social Security numbers** of their patients.

Washington University, MO / Mar 2017 / [Story](#)

University of Wisconsin Health **had over 2,000 patients' information compromised** after an **employee's email account was used by an unauthorized user**.

University of Wisconsin, WI / Mar 2017 / [Story](#)

**A data breach involving financial aid forms** at Daytona State College **exposed PII of students and their parents.** This breach was discovered while investigating a **separate breach of employee W-2s.**

Daytona State College, FL /  
Mar 2017 / [Story](#)

A **virus-infected computer** at the Lane Community College health clinic may have **relayed patient information including names, addresses, Social Security numbers and more to an unknown third party** for more than a year.

Lane Community College, OR /  
Mar 2017 / [Story](#)

A University of Idaho **employee's e-mail address was hacked and used to send phishing e-mails** to other employees. The e-mail requested the employees log in to what appeared to be an Office 365 Portal.

University of Idaho, ID /  
Mar 2017 / [Story](#)

**More than 7,000 patients** of West Virginia University Medicine University Healthcare had their **PHI breached** when an **employee accessed patient information** without authorization. **Over 100 of these patients have been victims of identity theft.**

WVU Medicine, WV /  
Feb 2017 / [Story](#)

## Financial Loss

Coastal Carolina University sent over \$1,000,000 to a scammer posing as a vendor. The university **employee fell for a phishing e-mail scam** requesting a change the company's bank account information.

Coastal Carolina University, SC / Mar 2017 / [Story](#)