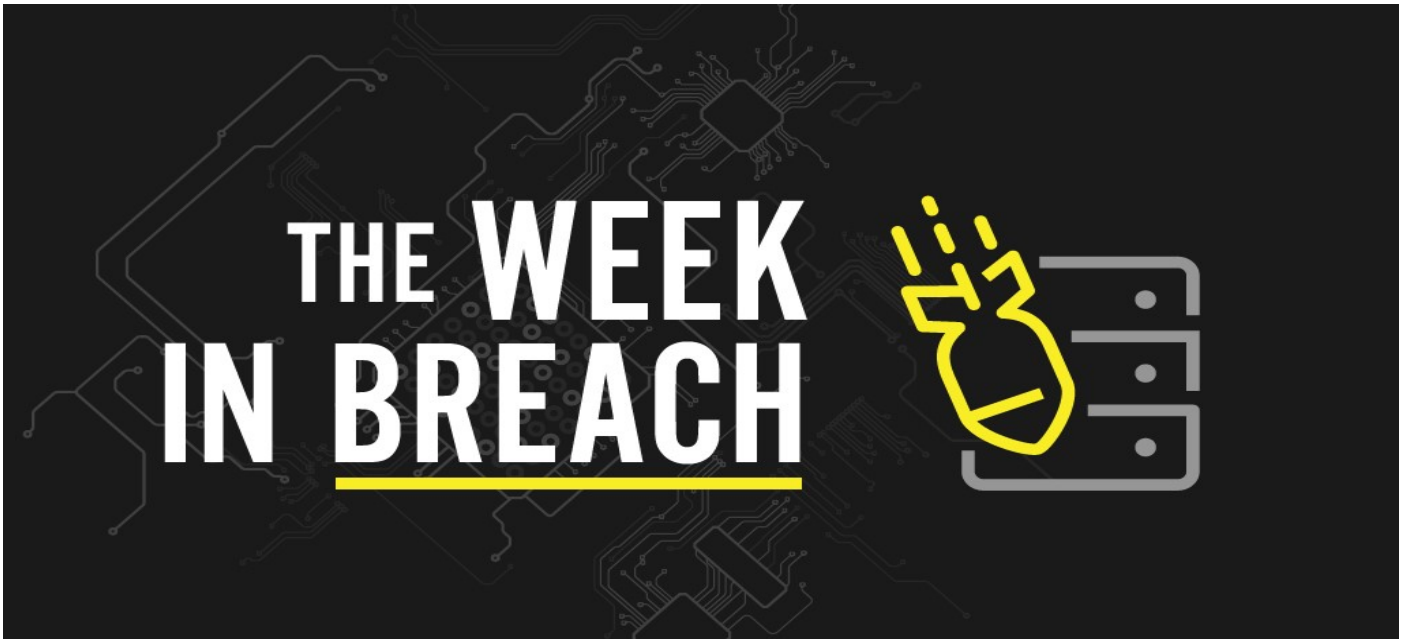
THE WEEK IN BREACH NEWS: 09/01/21— 09/07/21

DenBe Computer Consulting
Connecting Business

September 8, 2021 by Dennis Jock

Two COVID-19 contact tracing and testing platform breaches show a continuing trend in that area, Fujitsu had data debut on the dark web and a look at how ransomware targets are chosen – is your client next?



If your business isn't using our ***Dark Web Monitoring Services*** please call us for a free scan and to discuss setting up this cutting edge monitoring service for you!

Not ready to talk yet? Visit our website to get your ***FREE Dark Web Scan.*** You will get a free, no obligation scan sent to your inbox within 24hrs. ***Visit today: www.denbeconsulting.com***

United States: Pacific City Bank

https://securityaffairs.co/wordpress/121872/cyber-crime/pacific-city-bank-avos-locker-ransomware.html

Exploit: Ransomware

Pacific City Bank: Financial Institution

Risk to Business: **1.623 = Severe**

Pacific City Bank, a California-based bank that focuses on the Korean-American community, was rocked by ransomware. The bank was hit by the AVOS Locker ransomware gang last week. On Saturday, September 4, 2021, the ransomware gang added the bank to its leak site and published some screenshots as proof of the hack including a ZIP archive that contains a series of documents allegedly stolen from the bank. The incident is under investigation.

Individual Impact: No information was available at press time to say if employee, customer or consumer financial details or PII was compromised in this incident but since it is a bank that's highly likely.

Customers Impacted: Unknown

How It Could Affect Your Business: Ransomware gangs have been hungry for financial industry data and they've been stepping up attacks against targets that have it, especially small-time players that tend to have weak security.

United States: DuPage Medical Group

https://www.chicagotribune.com/business/ct-biz-dupage-medical-group-breach-personal-information-20210830-frv74cy23nhftgufbwc3caknie-story.html

Exploit: Hacking

DuPage Medical Group: Healthcare Practice

Risk to Business: **1.636 = Severe**

DuPage Medical Group is notifying 600,000 patients that their personal information may have been compromised during a July cyberattack. The largest independent physician group in Illinois experienced a computer and phone outage that lasted nearly a week in mid-July. Investigators determined that the incident was caused by unauthorized actors who accessed its network between July 12 and July 13.

Individual Risk: **1.866 = Severe**

The investigators determined that files containing patient information including names, addresses, dates of birth, diagnosis codes, codes identifying medical procedures and treatment dates may have been exposed. For a small number of people, Social Security numbers may have been compromised.

Customers Impacted: 600,000 patients

How it Could Affect Your Business: Exposed medical data isn't just a disaster upfront. Big penalties from state and federal regulators can cause damage that's hard to recover from.

United States: Career Group, Inc

https://www.securityweek.com/recruiting-firm-apparently-pays-ransom-after-being-targeted-hackers

Exploit: Ransomware

Career Group, Inc.: Staffing Company

Risk to Business: 1.673=Severe

California-based staffing service Career Group, Inc. Experienced a data breach, between June 28 and July 7. In the company's letter to regulators, it stated that it had received assurances from the cybercriminals involved that its data would be deleted, indicating a probable ransomware incident.

Individual Risk: 1.673=Severe

The company noted in a letter to the Maine Attorney General's Office the fact that the stolen data included PII from applicants and placements including Social Security numbers, but no further details were available at press time.

Customers Impacted: 49,476

How it Could Affect Your Business: Staffing services are a goldmine for cybercriminals because they offer the opportunity to quickly score a large amount of desirable financial data and PII.

United States: Howard University

Exploit: Ransomware

Howard University: Institution of Higher Learning

Risk to Business: **1.917 = Severe**

Howard University announced that they are investigating a ransomware attack. The incident disrupted online classes for several days. In person instruction was unaffected. The school's Enterprise Technology Services (ETS) intentionally shut down the university's network to investigate. So far, investigators have not found that any personal data on staff or students has been stolen.

Individual Impact: No information was available at press time about the types of data that was stolen if any.

Customers Impacted: Unknown

How it Could Affect Your Business: Medical data is a big revenue driver for cybercriminals but it is an even bigger revenue disaster for the medical practices that lose it to cybercrime.

France: Francetest

https://www.connexionfrance.com/French-news/700000-French-pharmacy-Covid-test-results-left-publicly-available

Exploit: Misconfiguration

Francetest: COVID-19 Test & Trace Platform

Risk to Business: 1.721 = Severe

A misconfiguration in an online platform used to transfer data from antigen tests carried out at pharmacies to the government platform SI-DEP has made hundreds of thousands of COVID-19 test results public, along with the PII of the patients who took them. In a particularly interesting detail of this story, the misconfiguration was discovered when a patient with IT expertise discovered that the open-source content management system WordPress was being used to manage sensitive data. She could access files containing other patients' information via the URL tree and even create an account without being a pharmacist.

Individual Risk: 1.761 = Severe

Exposed data included patients' full names, genders, dates of birth, social security numbers, contact details (including email address, telephone number and postal address) and test results including COVID-19 status.

Customers Impacted: 70,000

How it Could Affect Your Business: Human error is still the biggest cause of a data breach and this is one mistake that's going to cost a fortune by the time GDPR penalties are calculated.

France: France-Visas

https://www.connexionfrance.com/French-news/Personal-details-of-8-700-French-visa-applicants-exposed-by-hackers

Exploit: Hacking

France-Visas: Government Services Platform

Risk to Business: 1.919 = Severe

A cyber-attack has compromised the data of around 8,700 people applying for visas to visit or move to France via the official government-run France-Visas website. No details of the nationalities affected or other information about the applicants that had information exposed was released, but French officials say that they have been contacted by mail.

Individual Risk: 1.778 = Severe

Applicant PII including names, passport and identity card numbers, nationalities and birth dates was snatched by the hackers. No financial information was exposed. Officials noted a low potential for misuse because of strict GDPR compliance procedures.

Customers Impacted: 8,700

How it Could Affect Your Business: Their compliance may be stringent, but their security is lacking, and that's going to cost a pretty penny when penalties are handed down from GDPR regulators.

Japan: Fujitsu

https://www.zdnet.com/article/fujitsu-says-stolen-data-being-sold-on-dark-web-related-to-customers/

Exploit: Hacking

Fujitsu: Information Technology

Risk to Business: 1.802 = Severe

Data from Japanese tech giant Fujitsu is being sold on the dark web. The type of data available is unclear, but the cybercriminals responsible for the hack claim to have 4GB of company data to offload. In their announcement, the cybercriminals provided samples of the data and claimed they had confidential customer information, company data, budget data, reports and other company documents, including project information.

Individual Impact: No information was available at press time to say if employee, customer or consumer financial details or PII was compromised in this incident.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is the weapon of choice for both run-of-the-mill cybercriminals and nation state threat actors. Every business needs to be ready for it.

Indonesia: Electronic Health Alert Card

https://www.zdnet.com/article/passport-info-and-healthcare-data-leaked-from-indonesias-covid-19-test-and-trace-app-for-travellers/

Exploit: Misconfiguration

electronic Health Alert Card (eHAC): COVID-19 Test & Trace Platform

Risk to Business: 1.802 = Severe

A storage snafu has exposed a big pool of personal data from Indonesia's test and trace tool electronic Health Alert Card (eHAC). Researchers discovered that an unsecured Elasticsearch database was being used to store over 1.4 million records from approximately 1.3 million eHAC users. Both foreigners and Indonesian citizens must download the app, even those traveling domestically within the country and it contains data personal data for travelers including a person's health status, personal information, contact information, COVID-19 test results and other information.

Individual Risk: 1.5882 = Severe

The data involved in the leak includes user IDs including passports and national Indonesian ID numbers, COVID-19 test results and data, hospital IDs, addresses, phone numbers, URN ID numbers and URN hospital ID numbers. For Indonesians, their full names, numbers, dates of birth, citizenship, jobs and photos were included in the leaked data. Private information about Indonesian hospitals and government officials who used the app was also exposed.

How it Could Affect Your Business: A misconfiguration of this scale is embarrassing and demonstrates a slapdash security system that won't fill users with confidence.