akron bar association®

Data Breaches: How They Happen & an Update on Ohio & California Law

Andrew Jaffe, Esq.

Data Breaches: How they Happen & an Update on Ohio & California Law

Andrew M. Jaffe
Attorney at Law
Practice Limited to E-Commerce & Internet Law
2375 Covington Rd. Suite 315
Akron, Ohio 44313
(330) 983 -4842
attorneyjaffe@aol.com
www.LawyerJaffe.com

There Is No Gravity On The Internet – What Goes Up Does Not Come Down

PRIVACY AND THE INTERNET

General Data Protection Regulation (GDPR)

Data Control Officer

What is a Data Breach?

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

What is Personally identifiable information (PII)

1.First and last name;
2. Home or other physical address, including street name and name of a city or town;
3. Email address;
4. Telephone number;
5. A government issued identifier (e.g. Drivers license) ;
6. Biometric Identifiers (e.g. fingerprint or eye scan);
7. Any complete login information (which is usually a big surprise to the client.); or
8. An individual's name plus one or more of the following: a) Social security number, b) Driver's license or State identification card number, c) Financial account numbers, d) Medical information or e) Health insurance information.
9. Any other identifier that permits the physical or online contacting of a specific individual.

7 different types of data breaches

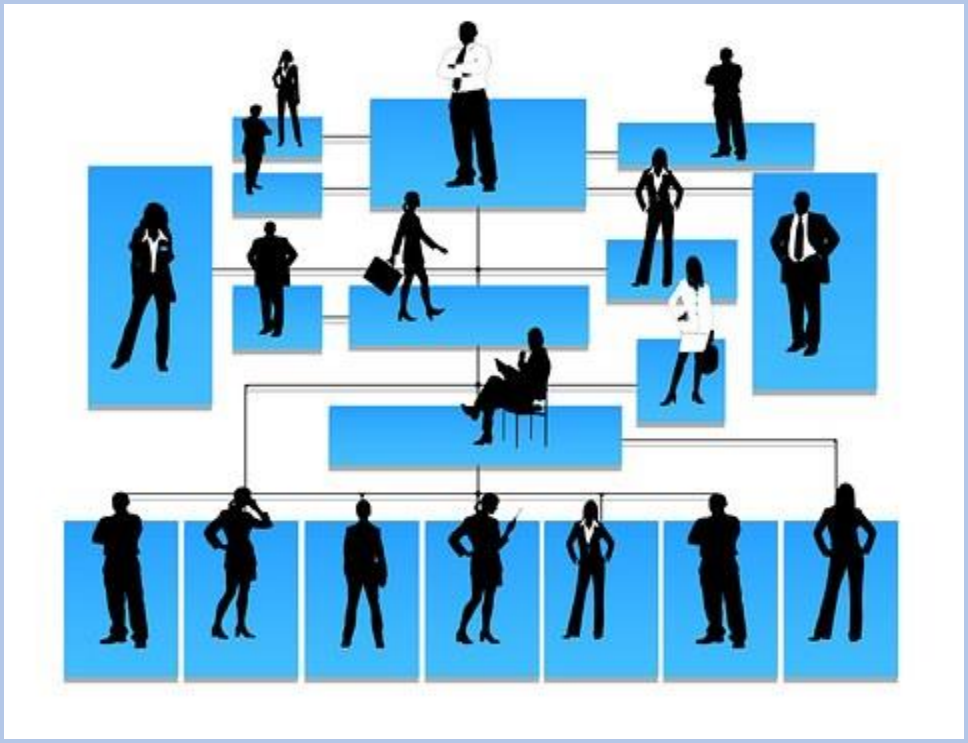
1. Cyber attack/criminal hacker

7 different types of data breaches

2. Employee negligence/error

7 different types of data breaches

3. Unauthorized access



7 different types of data breaches

4. Physical theft/exposure

7 different types of data breaches

5. Ransomware

7 different types of data breaches

6. Insider threat

7 different types of data breaches

7. Phishing

Don’t Be Dumb About Your Smart Phone - Courts Recognize A Smart Phone As A Computer

- Let us consider this scenario. You go out to lunch and forget to pick your phone up off the table. You get home and go to call someone a couple of hours later and cannot find your phone. You call the phone to try and find it, but do not hear it ring. You go out and look in your car, and don’t find it there. You figure it will show up and wait a day or two until you call your provider to shut the phone down. finally, you realize you have lost your phone and you are going to need to buy a new one – adding to your aggravation.
- Here are the problems you face because you did not have your phone password protected. First of all, your phone is a computer. It contains apps for your convenience, perhaps even your banking information. Someone who found your unlocked phone has had a day or two to use those apps and run up your bills. They may even have been able to buy things or take money from your accounts.
- Further, and maybe even more importantly, your contact list contains Personally Identifiable Information on a long list of people. If someone can access this list, you have now had a data breach from a computer. If you have people on your contact list who relate to your work, your company has now suffered a data breach. Your bosses will not be happy when you go to them and tell them the company needs to address a data breach – A situation that will cost the company not only embarrassment, but also considerable time and money to rectify.

The Average Cost of a Data Breach

Turns out the cost of data breaches and the volume of records stolen are only going up according to the 13th annual 2018 Cost of a Data Breach Study: Global Overview from IBM Security and Ponemon Institute.

The study reported that the global average cost of a data breach is $3.86 million, up 6.4 percent from last year. The average cost, globally, for each lost or stolen record containing sensitive and confidential information is also up from last year, landing at $148 per record. A 4.8 percent increase from 2017.

What are the biggest breaches to date?

The following table shows the 10 biggest breach incidents reported to date:

Company/Organization	Number of Records Stolen	Date of Breach
Yahoo	**3 billion**	August 2013
Equifax	**145.5 million**	July 2017
eBay	**145 million**	May 2014
Heartland Payment Systems	**134 million**	March 2008
Target	**110 million**	December 2013
TJX Companies	**94 million**	December 2006
JP Morgan & Chase	**83 million (76 million households and 7 million small businesses)**	July 2014
Uber	**57 million**	November 2017
U.S. Office of Personnel Management (OPM)	**22 million**	Between 2012 and 2014
Timehop	**21 million**	July 2018

If You Encrypt They Must Acquit

There are now Data Breach laws in all 50 States covering actions and notifications to be taken if there is a data breach. There is a 99% Save Harbor that there is no breach if the data is encrypted.

Ohio Data Breach Law

Ohio Rev. Code §§ 1349.19 – 192

Breach = Name + (1) social security number; (2) driver's license number or state identification card number; or (3) account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account. Plus, requires more than 1,000 residents are affected.

Notification to Individuals, Regulators & Credit Bureau

within 45 days

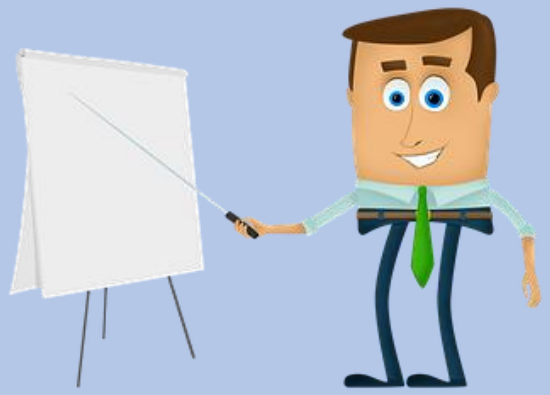
Ohio has the Encryption Safe Harbor

Data Breach Laws Require Notification

No matter where the breach occurred, notification is required by the State law where the individual lives, sometimes within 72 hours.

Cyber Security Tips for Small Business

1. Train employees in security principles
2. Protect information, computers, and networks from cyber attacks
3. Provide firewall security for your Internet connection
4. Create a mobile device action plan
5. Make backup copies of important business data and information
6. Control physical access to your computers and create user accounts for each employee
7. Secure your Wi-Fi networks
8. Employ best practices on payment cards
9. Limit employee access to data and information, limit authority to install software
10. Passwords and authentication



What To Do If There Is A Data Breach

1. I tell my clients I am their first call.
2. We will then hire a Data Forensic Specialist to learn exactly what was divulged.
3. We will inform the appropriate state agencies within the required time with a plan to protect the consumer.
4. Finally, we need to contact a PR firm to protect the Company's brand.

5. FTC's Data Breach Response: A Guide for Business

https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business-042519-508.pdf

ORC Chapter 1354 Ohio Law Offers Safe Harbor to Companies Meeting Cyber Standards

- As we all read in the news, data breaches seem to occur every day. Ohio has become the first state in the Union to create a "Safe Harbor" for businesses against tort claims if a data breach does occur.
- The Data Protection Act changes Ohio law so that businesses that take reasonable precautions and meet industry-recommended standards would be afforded a "safe harbor" against legal claims should a data breach occur. To trigger the "safe harbor" provision, businesses must create their own cybersecurity programs that meet certain standards. The legislation identifies eight different industry-recognized cybersecurity frameworks on which businesses can base their programs.
- As a data breach not only damages a business brand but costs the offenders no less than $100,000 and up to millions of dollars, businesses in Ohio should take the necessary steps to ensure their cybersecurity program meets the requirements of the Safe Harbor. While this will cost your business time and money, creating the Safe Harbor is well worth the time and expense to put the program in place.

The California Consumer Privacy Act of 2018

Effective Jan 1, 2020:

The CCPA applies to any business, including any for-profit entity that collects consumers' personal data, which does business in California, and satisfies at least one of the following thresholds:

- Has annual gross revenues in excess of $25 million;
- Possesses the personal information of 50,000 or more consumers, households, or devices; or
- Earns more than half of its annual revenue from selling consumers' personal information.

- Think Data Control Officer