Privacy and Data Security In Connecticut

Connecticut Office of the Attorney General
Privacy & Data Security Section
860.808.5440

Privacy and Data Security in Connecticut

1) AGO Privacy Section
2) Statutory Backdrop
3) AGO Breach Investigations
4) Current Breach Trends
5) Best Practices and Resources

Statutory Backdrop

- Connecticut Unfair Trade Practices Act
- Connecticut Safeguards Law
- Connecticut Cybersecurity Framework Law
- Connecticut Breach Notice Law

Connecticut Unfair Trade Practices Act (CUTPA):

Conn. Gen. Stat. § 42-110b, *et seq*.

No person shall engage in unfair or deceptive acts in the conduct of trade or commerce

Connecticut Unfair Trade Practices Act:

Penalties

Up to $5,000 per willful violation

Connecticut Safeguards Law:

Conn. Gen. Stat. § 42-471

- Requires any person in possession of personal information (PI) to safeguard data against misuse by third parties, and destroy, erase or make unreadable such data prior to disposal
- PI defined broadly as “information capable of being associated with a particular individual through one or more identifiers…”
- Electronic and paper records covered

Connecticut Safeguards Law:

Privacy Protection Policy

For SSNs, privacy protection policy must be published or publicly displayed.

Such policy shall:

- (1) protect SSNs;
- (2) prohibit unlawful disclosure of SSNs; and
- (3) limit access to SSNs

Connecticut Safeguards Law:

Penalties

$500 per intentional violation, up to $500,000 for single event

Connecticut Cybersecurity Framework Law:

Conn. Gen. Stat. § 42-901

- As of Oct. 1, 2021, businesses that follow recognized cybersecurity frameworks may be immune from punitive damages for tort claims in state court that arise from a data breach
- List of frameworks include, but are not limited to: NIST, ISO2700, as well as compliance with HIPAA and GLBA
- Cybersecurity program may vary based on: company size; nature and scope of activities; sensitivity of information; and cost/availability of security tools
- AGO enforcement actions are excluded from safe harbor

Connecticut Breach Notice Law:

Conn. Gen. Stat. § 36a-701b

Unauthorized access to or acquisition of Personal Information (PI) not secured by encryption or any other technology that renders PI unreadable

Connecticut Breach Notice Law:

What is Personal Information?

PI is a first name or first initial and last name along with:

- SSN;
- Driver's License number;
- Credit or debit card number; or
- Financial account number (with access code)

Connecticut Breach Notice Law:

What is Personal Information?

As of Oct. 1, 2021, PI also includes:

- Taxpayer ID number;
- IRS identity protection PIN;
- Passport number, military ID or other government ID;
- Certain medical information;
- Health insurance policy information;
- Biometric information; and
- Online account credentials

P.A. 21-59

Connecticut Breach Notice Law:

What is Required After a Data Breach?

- Notice to AGO and impacted Connecticut residents
- Notice must be made without “unreasonable delay”
- 60 day outside limit
- For compromised SSNs and ITINs, 2 years of ID theft prevention services required, such as credit monitoring

Connecticut Breach Notice Law:

Penalties

- *Per se* CUTPA violation
- Penalties: Up to $5,000 per violation

Connecticut Breach Notices 2012-2020

Statistics + Trends

Graph View

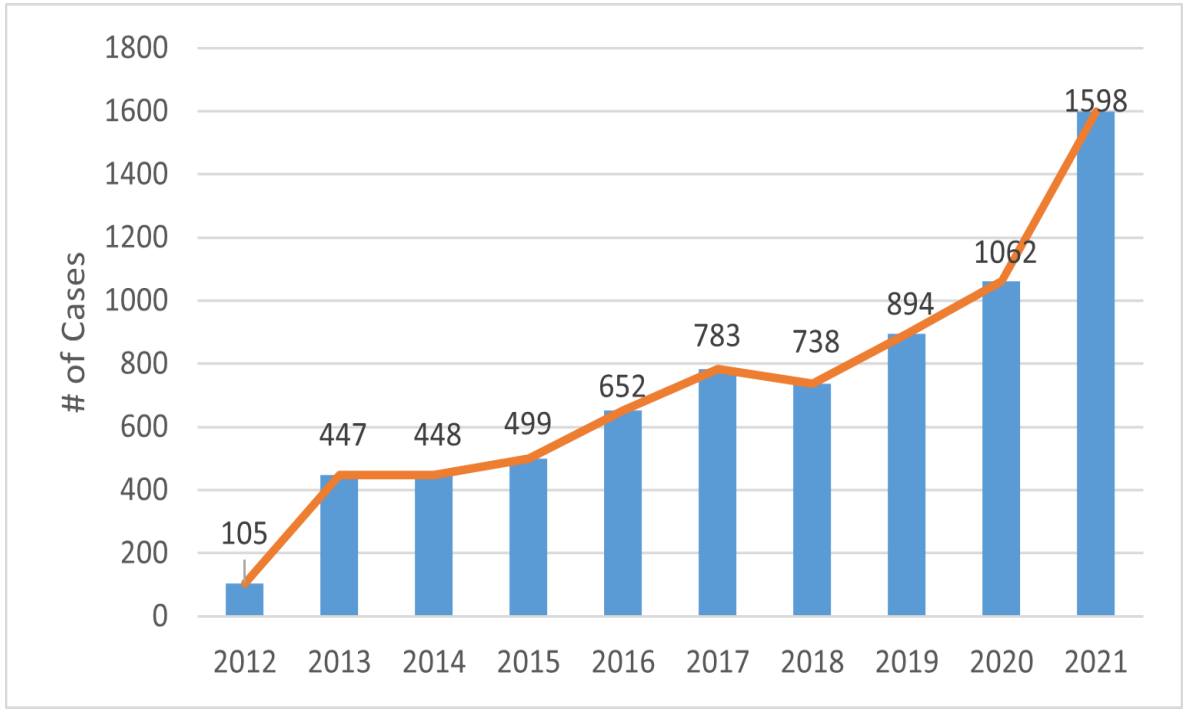

Table View

Year	Cases	YoY (in cases)	YoY %
2012	105		
2013	447	342	325.7%
2014	448	1	0.2%
2015	499	51	11.4%
2016	652	153	30.7%
2017	783	131	20.1%
2018	738	-45	-5.7%
2019	894	156	21.1%
2020	1062	168	18.8%
2021	1598	536	50.47

AGO Breach Investigations:

Recent Settlements & Key Takeaways

- **Equifax** ($600M): governance and data security must go hand-in-hand
- **Uber** ($148M): don't hide a breach
- **Anthem** ($39.5M): employee training is critical
- **Target** ($18.5M) and **Home Depot** ($17.5M): security is only as strong as weakest link

Current Breach Trends

- Ransomware
- Software Supply Chain Attacks
- Cloud Misconfigurations

Ransomware:

What is it?

- Ransomware is malware that locks access to a computer system or files by encrypting data; ransom demanded in exchange for decryption
- Sensitive data is often taken by the criminals during the attack and later sold on dark web
- Ransomware is lucrative and ransomware marketplaces have sprouted online

Ransomware Statistics

- Ransomware reports doubled in 2021.
  2021 Verizon Data Breach Investigations Report
- 37% of global organization were victims of a ransomware attack in 2021.
  IDC 2021 Ransomware Study
- In the first half of 2021, the FBI's IC3 reported 2,084 ransomware complaints -- a 62% year-over-year increase.
- In the first half of 2021, $590 million paid in ransom. *U.S. Treasury's Financial Crimes Enforcement Network*

Ransomware Targets

Ransomware can hit any industry – private and public entities of all sizes are targets.

Who is susceptible?

- Home-users
- Businesses
- Individuals
- Organizations

Anyone with important data stored on their computer or network is at risk.

Most commonly targeted sectors

CISA
CYBER+INFRASTRUCTURE

Ransomware:

How to Prevent and/ or Mitigate Attacks

- Back-up data and secure back-ups
- Segment network
- Update software/manage patches
- Implement anti-phishing controls
- Install access controls/MFA
- Prepare and test incident response plan (include current contact information)
  - Report attacks to local FBI field offices
  - File report w/ FBI's Internet Crime Complaint Center (IC3)

Software Supply Chain Attacks

- Supply chain attacks target software vendors or suppliers instead of directly targeting specific business; cybercriminals can then gain access to a host of sensitive business and customer information
- Supply chain attacks can be massive in scope and complex given the various business relationships
- How to prevent and mitigate:
  - Ensure vendors maintain best practices
  - Implement strong vendor access controls

Cloud Misconfigurations

- Shared responsibility model: both cloud service provider and user have obligations to secure data
- Misconfigurations are the most significant risk to cloud environment (and account for 60-70% of cloud breaches)
- How to prevent and mitigate:
  - Understand your responsibilities for cloud security
  - Educate team members about those responsibilities

Best Practices:

Cybersecurity

- **Minimize Data**: collect and keep only what you need; regularly review data retention policies and purge data
- **Take Stock**: conduct thorough asset inventories and risk assessments; mitigate risks
- **Train employees**: ensure workforce knows about privacy and security obligations; conduct mock phishing exercises and follow-up

Information security is everyone's responsibility

Best Practices:

Breach Notification

- **Be Upfront**: reach out to AGO and law enforcement early
- **Be Detailed**: ensure notices are drafted clearly and explain why consumers are receiving them
- **Be Prompt**: conducting a forensic investigation and identifying impacted individuals may take time, but do not ignore notice timeframes.

If SSNs or ITINs are compromised, offer CT residents 2 years of credit monitoring

Resources

- AGO Privacy Section: 860.808.5440
- AGO Breach Notification Portal
- CT Cybersecurity Resource Page
  - General tips
  - Sample cyber incident response plan
- CISA Ransomware Guide
  - Detailed best practices guide
  - Helpful ransomware response checklist
- CISA Incident Reporting Form
- Internet Crime Complaint Center
- National Cyber Investigative Joint Task Force - Ransomware Fact Sheet
- White House Memorandum on Ransomware