HIPAA Update from the Office for Civil Rights

Timothy Noonan
Deputy Director for Health Information Privacy, Data, and Cybersecurity
HHS Office for Civil Rights

Agenda

- HIPAA Rulemaking
- Trends in Large Health Data Breach Reporting
- Recent HIPAA Enforcement Activity

Policy

HIPAA Privacy Rule to Support Reproductive Health Care Privacy Final Rule

- Strengthens privacy protections by prohibiting the use or disclosure of PHI by a regulated entity for either of the following purposes:
  - To conduct a criminal, civil, or administrative investigation into or impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care that is lawful under the circumstances in which it is provided.
  - The identification of any person for the purpose of conducting such investigation or imposing such liability.

- Prohibition applies where the regulated entity has reasonably determined that one or more of the following conditions exists:
  - The reproductive health care is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided.
  - The reproductive health care is protected, required, or authorized by Federal law, including the U.S. Constitution, regardless of the state in which such health care is provided.
  - The reproductive health care was provided by a person other than the regulated entity that receives the request for PHI and the presumption of lawfulness (next slide) applies.

HIPAA Privacy Rule to Support Reproductive Health Care Privacy Final Rule (cont'd)

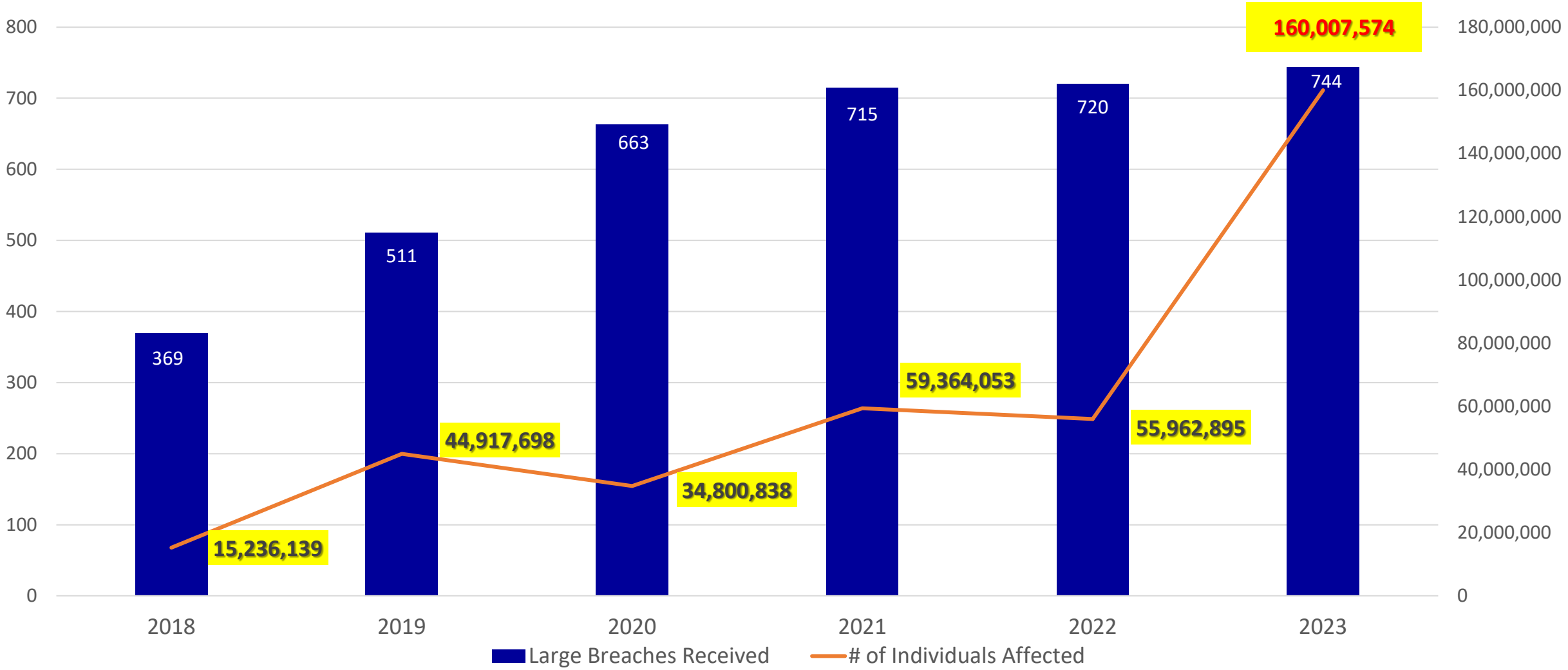
- Reproductive health care provided by a person other than the regulated entity that receives the request for PHI is presumed lawful unless the regulated entity has any of the following:
  - Actual knowledge that the reproductive health care was not lawful under the circumstances in which it was provided.
  - Factual information supplied by the person requesting the PHI that demonstrates to the regulated entity a substantial factual basis that the reproductive health care was not lawful under the specific circumstances in which it was provided.
- Before a regulated entity responds to certain requests for PHI potentially related to reproductive health care, it must obtain an attestation from the person requesting the PHI that the requested use or disclosure is not for a prohibited purpose. Applies when the request for PHI is for:
  - Health oversight activities
  - Judicial and administrative proceedings
  - Law enforcement purposes
  - Disclosures to coroners and medical examiners

HIPAA Privacy Rule to Support Reproductive Health Care Privacy Final Rule (cont'd)

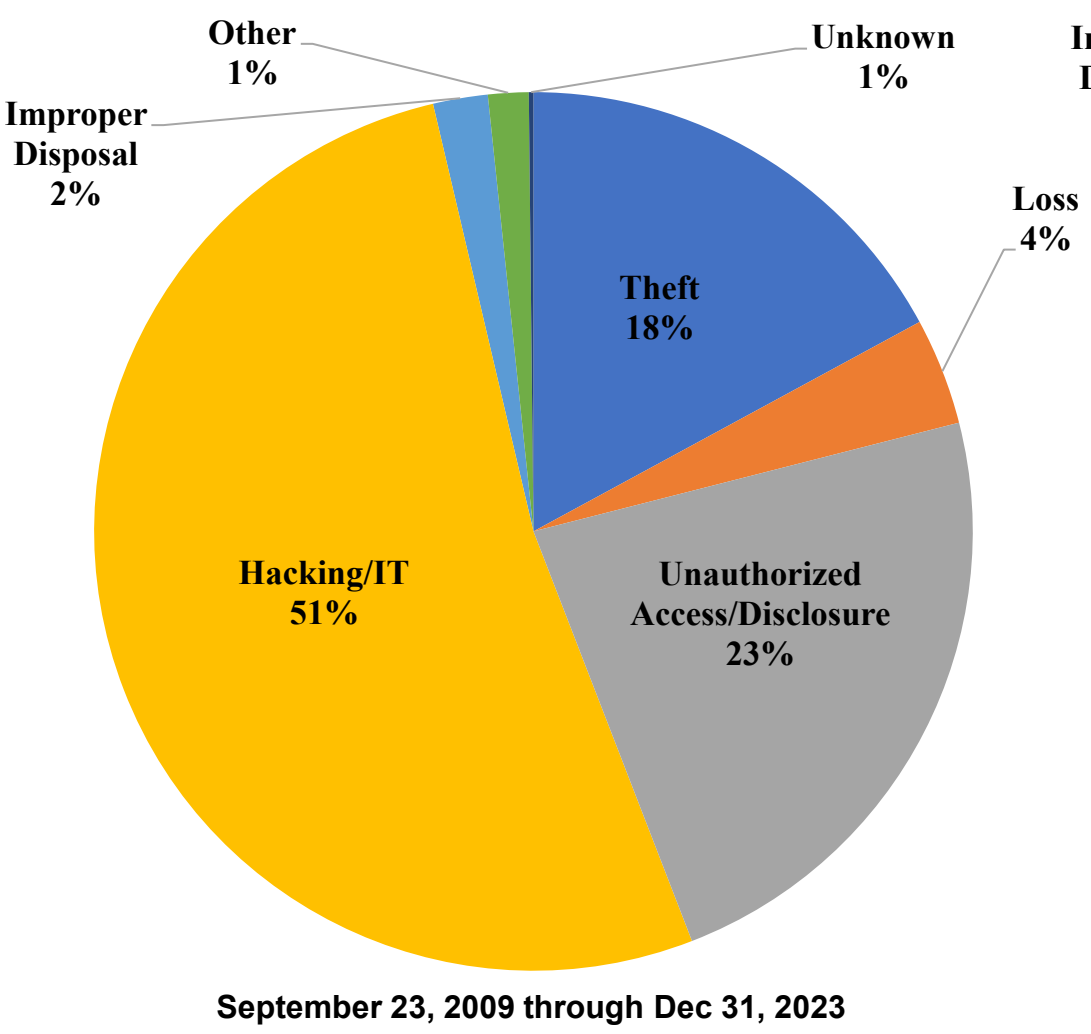
- Resources
  - Final Rule: https://www.federalregister.gov/documents/2024/04/26/2024-08503/hipaa-privacy-rule-to-support-reproductive-health-care-privacy
  - Fact Sheet: https://www.hhs.gov/hipaa/for-professionals/special-topics/reproductive-health/final-rule-fact-sheet/index.html
  - Model Attestation: https://www.hhs.gov/sites/default/files/model-attestation.pdf
  - Webinar: https://www.youtube.com/watch?v=L6O0jnqoA78
  - Social Media Toolkit: https://www.hhs.gov/sites/default/files/social-media-toolkit-hipaa-reproductive-health-care-privacy.pdf
  - OCR Director Message (English): https://www.youtube.com/watch?v=2YMBPdkCPqk
  - OCR Director Message (Spanish): https://www.youtube.com/watch?v=jSTuiIZdIEg

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

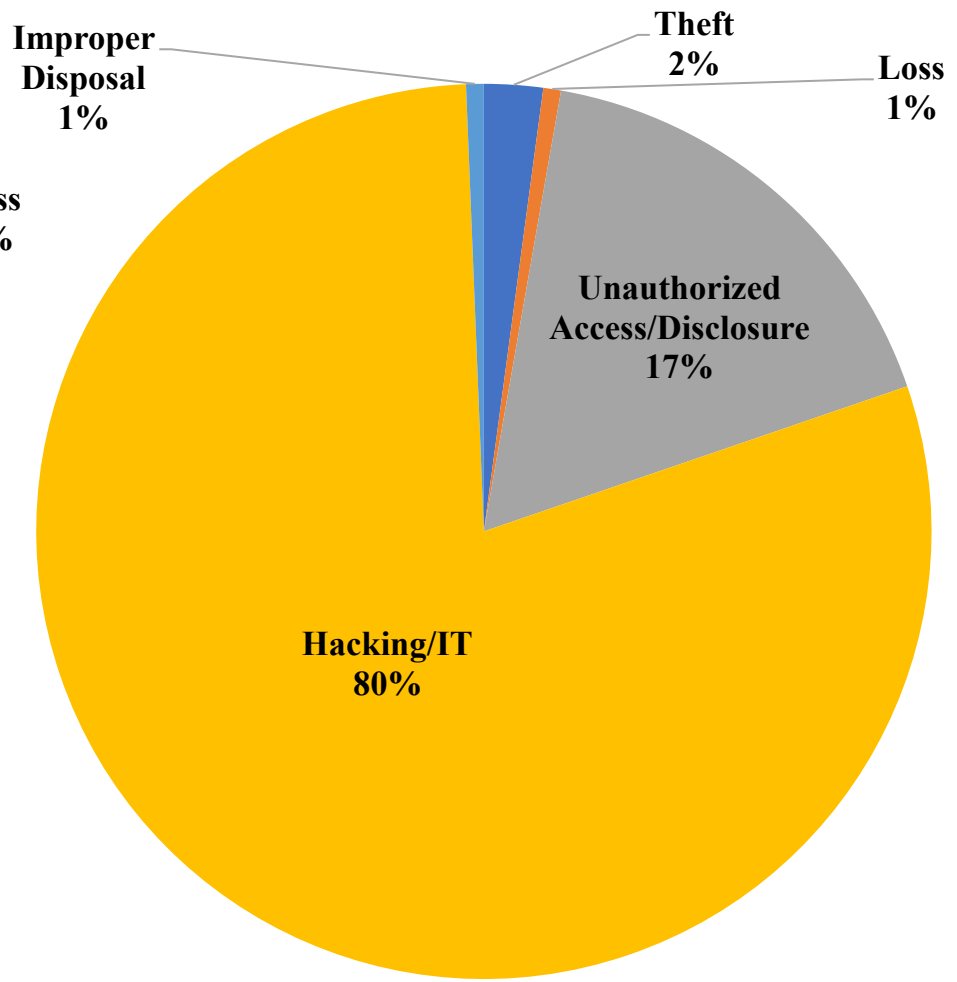
Large Breaches Received and # of Individuals Affected 2018 - 2023



500+ Breaches by Type of Breach



September 23, 2009 through Dec 31, 2023

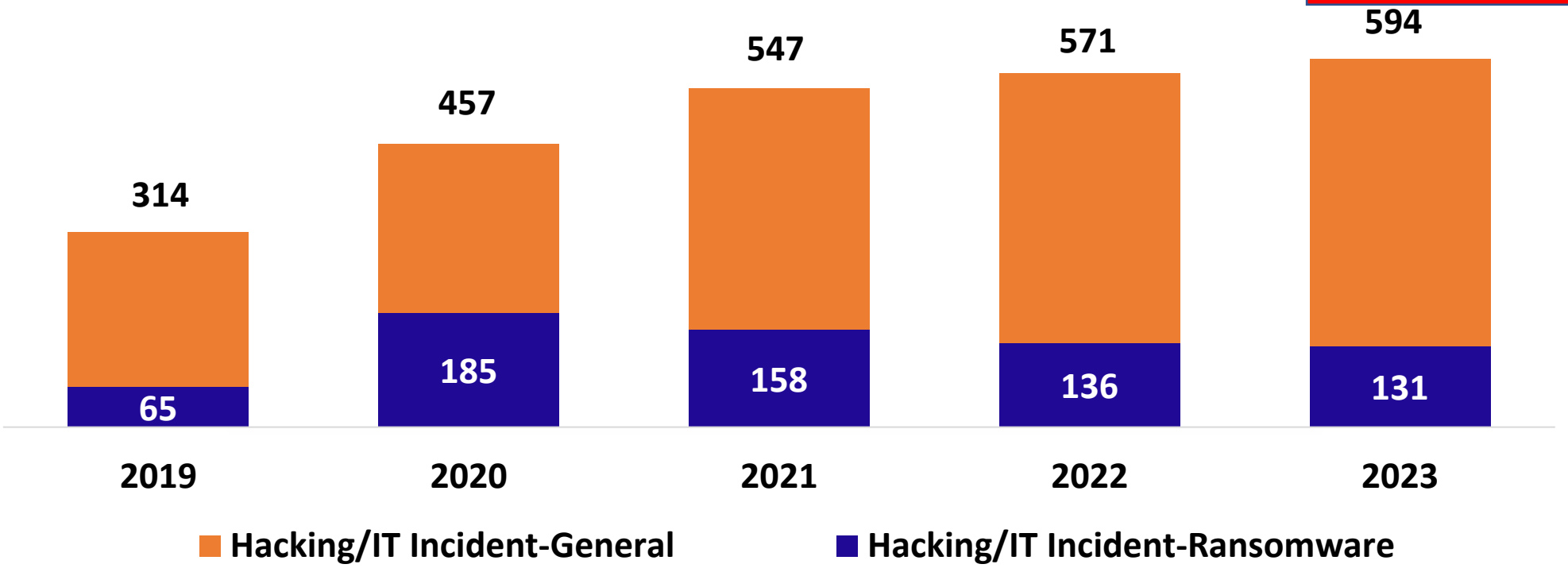


January 1, 2024 through August 31, 2024

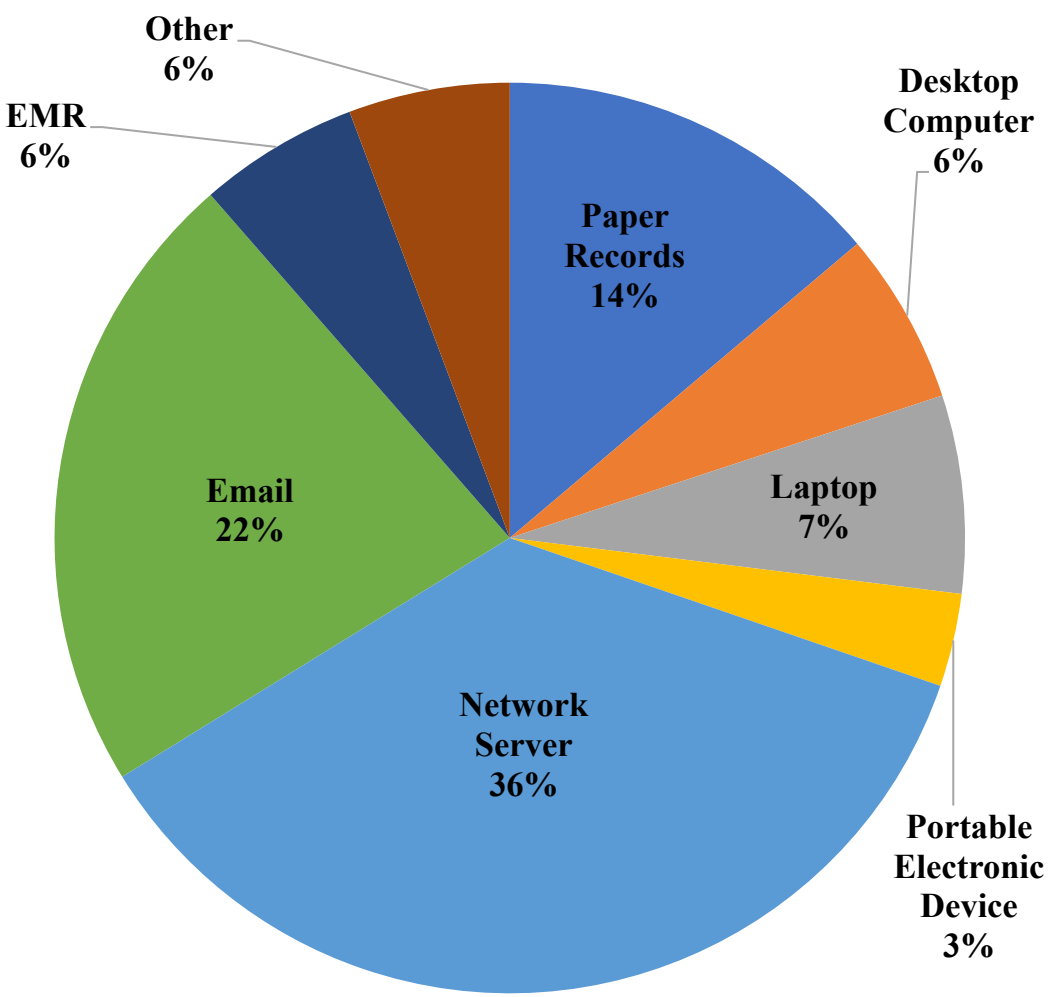
Breaches Affecting 500 or More Individuals
Reports Received Involving Hacking/IT Incidents

Calendar Years 2019 - 2023

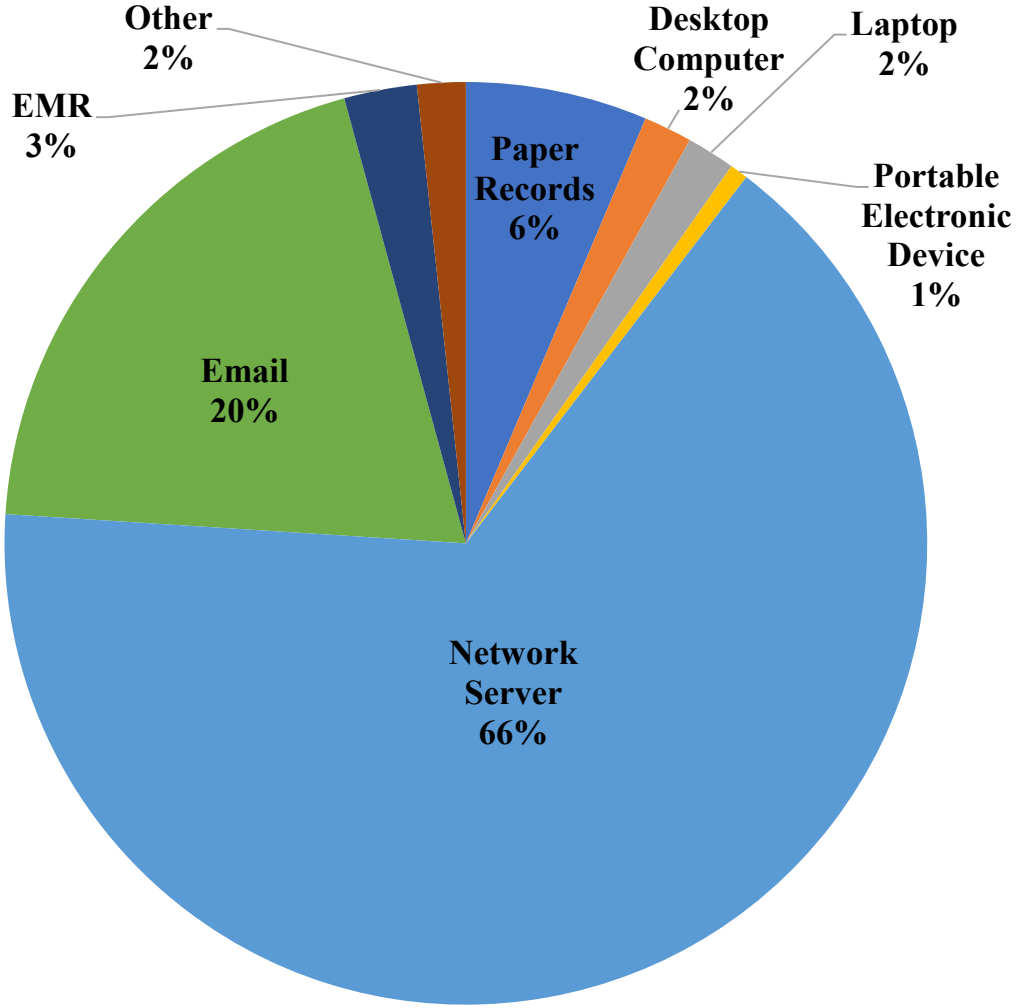
2019 - 2023
89% increase in hacking
102% increase in ransomware



500+ Breaches by Location of Breach



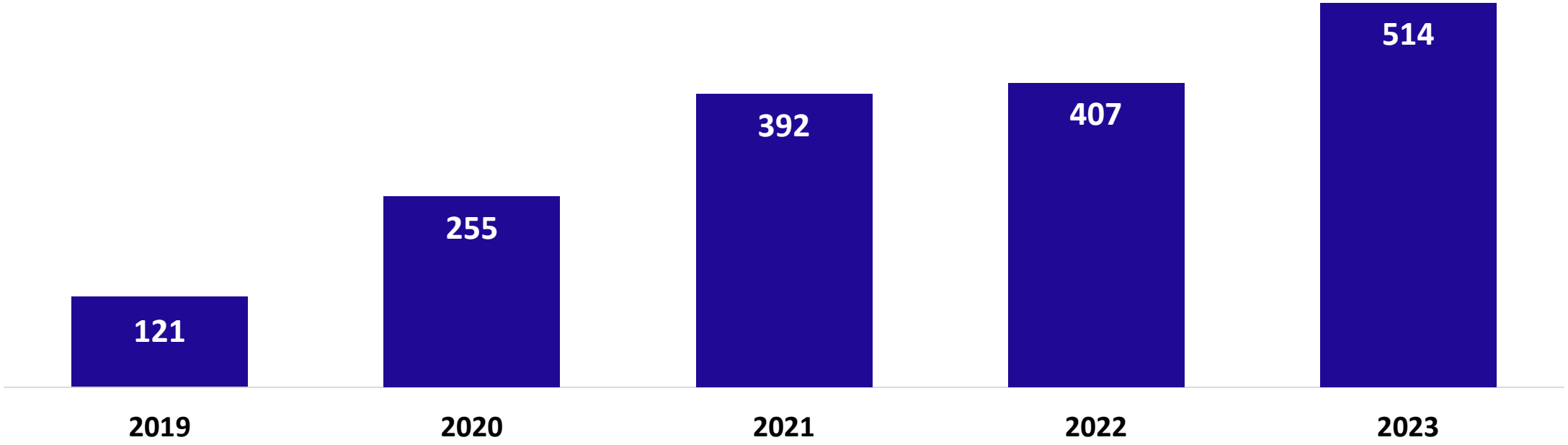
September 23, 2009 through Dec 31, 2023



January 1, 2024 through August 31, 2024

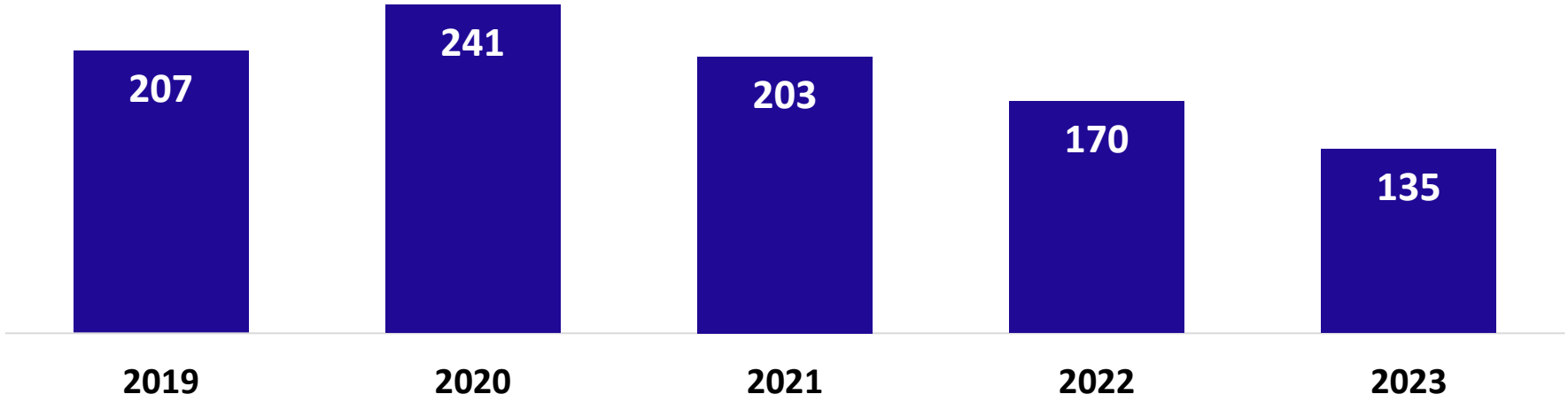
Breaches Affecting 500 or More Individuals
Reports Received of Breaches Involving Network Servers

Calendar Years 2019 - 2023



Breaches Affecting 500 or More Individuals
Reports Received of Breaches Involving Email Accounts

Calendar Years 2019 - 2023



Recent Announced OCR HIPAA Enforcement Actions

Aug-23	United Healthcare Insurance Company	$80,000
Sep-23	LA Care Health Plan	$1,300,000
Oct-23	Doctors' Management Services	$100,000
Nov-23	St. Joseph's Medical Center	$80,000
Dec-23	Lafourche Medical Group	$480,000
Jan-24	Optum Medical Care of New Jersey	$160,000
Feb-24	Montefiore Medical Center	$4,750,000
Feb-24	Green Ridge Behavioral Health, LLC	$40,000
Mar-24	Phoenix Healthcare	$35,000
Apr-24	Essex Residential Care, LLC	$100,000
July-24	Heritage Valley Health System	$950,000
Aug-24	American Medical Response	$115,200