Buchanan

Last Updated December 2025

US Privacy and Security Enforcement Report

Table of Contents

Page

ADMINISTRATIVE REMEDIES

The Gramm-Leach-Bliley Act (GLBA), Title V, 15 U.S.C. §§6801-6809 and its implementing regulations: The Federal Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) as well as federal functional regulators and state insurance authorities have the power to enforce GLBA with respect to the entities within a particular agency's authority. The CFPB can initiate administrative adjudication enforcement actions against potential violators. The CFPB has established the Office of Administrative Adjudication, which is an independent judicial office within the CFPB. The CFPB has the power to issue cease and desist orders, following notice to the alleged violator and a scheduled hearing. The CFPB also has the power to undertake investigations of a potential violator by issuing a civil investigative demand. As part of its investigation, the CFPB can issue demands for production of documents as well as for giving oral testimony.

Section 5 of the Federal Trade Commission Act, 15 USC §45 (FTC Act): The FTC may bring an administrative hearing against an individual or entity suspected of unfair or deceptive trade practices in violation of the FTC Act. At the conclusion of such a hearing, the FTC may issue an order to cease and desist. If the individual or entity subject to the order violates that order, the FTC may issue administrative penalties of up to **$53,088 per violation**.

The Children's Online Privacy Protection Rule, 16 CFR 312.1 et. seq., implementing the Children's Online Privacy Protection Act of 1998, 15 USC §6501 et. seq. (COPPA): Violations of COPPA are deemed to be unfair or deceptive trade practices and are therefore subject to the same administrative penalties as set forth under the FTC Act, as described above. COPPA also gives states and certain other federal agencies authority to enforce compliance.

The Health Insurance Portability and Accountability Act of 1996, as amended and implemented at 45 C.F.R. Parts 160, 162, and 164 (HIPAA): The Department of Health and Human Services (HHS), through its Office for Civil Rights (OCR), enforces the privacy and security requirements of HIPAA. If an investigation indicates that a regulated entity (Covered Entities and Business Associates) was not in compliance, OCR will seek to resolve the investigation with voluntary compliance, corrective action, or a resolution agreement.

U.S. State Breach, Privacy, and Security Laws: The U.S. also has significant privacy and security regulation at the state level. All states (including Washington D.C.) have a law requiring notification in the event of a breach of security of personal information. Such duties are typically triggered by the unauthorized access or acquisition of personally identifiable information, and notice to the affected individuals, state authorities, and credit reporting agencies may be required. Several states also impose strict requirements regarding the information security standards of businesses that maintain personally identifiable information. The state attorney general is most commonly the enforcement authority for these laws and may have the ability to investigate or bring actions for an injunction and/or civil penalties.

CIVIL REMEDIES

GLBA: The FTC has the power to bring civil action for damages. Penalties include rescission or reformation of contracts; monetary refunds or return of real property; restitution; disgorgement or compensation for unjust enrichment; monetary penalties; public notification of the violation; and limits on the violator's functions. Civil monetary penalties range from a maximum of $5,000 per day of violation to $1,000,000 per day of violation, where an individual knowingly violated the law.

FTC Act: The FTC may bring civil actions for civil monetary penalties of up to **$53,088** per violation. Each day that non-compliance continues is considered a separate "violation" for purposes of the law.

COPPA: Violations of COPPA are deemed to be unfair or deceptive trade practices and are therefore subject to the same civil remedies as set forth under the FTC Act, as described above. COPPA also gives states and certain other federal agencies authority to enforce compliance.

HIPAA: OCR may impose a civil monetary penalty on any person who violates HIPAA's requirements, at an amount of between US $100 to 50,000 per violation, with a total of US $25,000 to 1.5 million for all violations of a single requirement in one calendar year. The Health Information Technology for Clinical and Economic Health Act (HITECH) also gives state attorneys general the authority to bring civil actions on behalf of state residents for violations of HIPAA and obtain damages on behalf of residents or enjoin further violations of HIPAA.

U.S. State Breach, Privacy, and Security Laws: As mentioned above, state Attorneys General have been active in enforcing federal and state privacy and cybersecurity laws. For example, if the Attorney General of New York brings an action for a violation of that state's breach notification law, the court may impose a civil penalty of up to $150,000. In Texas, the Attorney General announced earlier this year a settlement against a global search engine provider for unlawfully tracking and collecting users' private data, including geolocation, incognito searches, and biometric information. That company agreed to pay **$1.375 billion**. And while this is just one example, penalties vary widely by jurisdiction.

CRIMINAL REMEDIES

GLBA: While the CFPB has no power itself to bring criminal actions, pursuant to federal statute, if the CFPB obtains evidence that a person has engaged in conduct that may violate a federal criminal law, the CFPB is authorized to provide that evidence to the Attorney General of the United States, who will be able to investigate and potentially bring an enforcement action.

FTC Act: No criminal penalties specified.

COPPA: No criminal penalties specified.

HIPAA: Violations of HIPAA can include criminal penalties, including up to ten years imprisonment in certain cases. These penalties may be imposed on Business Associates as well as Covered Entities, as defined under the law.

U.S. State Breach, Privacy, and Security Laws: State laws do not typically provide criminal penalties for violations.

OTHER REMEDIES

The Telephone Consumer Protection Act of 1991 (TCPA), codified as 45 U.S.C. §227: The TCPA regulates certain telemarketing practices and prohibits unsolicited marketing faxes as well as calls and text messages placed by auto-dialers or using prerecorded voices. It also imposes certain limitations on the times which solicitors can call residences and requires solicitors to adhere to the National Do Not Call (DNC) Registry as well as maintain their own DNC lists. The TCPA provides consumers with a private right of action of up to $1,500 for each willful violation.

U.S. State Breach, Privacy, and Security Laws: In addition to enforcement by the state attorneys general, many states allow individuals to bring private suits for violations. For example, New Hampshire law permits individuals injured under its breach notification statute to bring an action for damages and equitable relief (such as an injunction), as deemed appropriate by the court.

SELECTED ENFORCEMENT ACTIONS

Federal Communications Commission:

- In August 2025, the FCC issued a **Final Removal Order**, removing over 1,200 voice service providers from its Robocall Mitigation Database for failing to certify their robocall mitigation efforts. This Order aimed at tackling illegal robocalls will effectively disconnect these voice service providers from the U.S. phone network.[1]

- In September 2024, the FCC entered into a **$13 million** settlement with *AT&T* to settle charges that AT&T failed to protect the confidentiality of consumers' personal information when it failed to ensure its cloud vendor adequately protected customer information.[2]

- In July 2024, the FCC entered into a **$16 million** settlement with *TracFone*, a United States-based wireless prepaid service provider, to settle charges that TracFone violated The Communications Act of 1934 when it failed to take measures to protect customer data. TracFone's failure allowed third-party actors

[1] *See* FCC, https://docs.fcc.gov/public/attachments/DA-25-737A1.pdf, (enforcement order released Aug. 25, 2025).
[2] *See* FCC, https://docs.fcc.gov/public/attachments/DA-24-892A1.pdf, (enforcement order released Sep. 17, 2024).

to gain access to customer information such as customer names and billing addresses. [3]

- In March 2016, the FCC announced a settlement of **$1.35 million** with a telecommunications provider over allegations that it had used unique, undeletable identifiers (supercookies) without the knowledge or consent of consumers. The provider was also required to adopt a three-year compliance plan.[4]

- In July 2015, the FCC entered into a **$3.5 million** settlement with two telecommunications providers resolving its investigation of those entities. Specifically, the FCC investigation had focused on whether the companies had failed to protect the confidentiality of personal information received from more than 300,000 customers. The FCC had also been investigating whether one of the providers had failed to comply with its instructions to remove ineligible subscribers.[5]

- In November 2015, the FCC entered into a **$595,000** settlement with a communications company resolving its investigation into whether the company had failed to properly protect customers' personal information when its data systems were breached in 2014.[6]

- In April 2015, *AT&T* entered a **$25 million** settlement with the Federal Communications Commission to resolve an investigation into consumer privacy violations at some of AT&T's international call centers. AT&T was also required to implement an information security program, appoint a senior compliance manager, conduct a privacy risk assessment, and provide ongoing training to employees on the company's privacy policies.[7]

- In May 2014, *Sprint* entered into a **$7.5 million** settlement to resolve an investigation into the company's failure to honor consumers' do-not-call or do-not-text requests. The company had independently discovered that human error and technical malfunction resulted in telemarketing calls and texts to unauthorized numbers. In addition to the monetary penalty, the FCC required Sprint to implement a compliance plan, appoint a compliance officer, and establish a compliance training program.[8]

[3] *See* FCC, https://docs.fcc.gov/public/attachments/DA-24-481A1.pdf (enforcement order released Jul. 22, 2024).
[4] https://apps.fcc.gov/edocs_public/attachmatch/DOC-338091A1.pdf.
[5] https://apps.fcc.gov/edocs_public/attachmatch/DOC-334286A1.pdf.
[6] https://apps.fcc.gov/edocs_public/attachmatch/DOC-336222A1.pdf.
[7] *See* FCC Press Release, https://apps.fcc.gov/edocs_public/attachmatch/DOC-332911A1.pdf.
[8] *See* FCC Order and Consent Decree, https://apps.fcc.gov/edocs_public/attachmatch/DA-14-527A1.pdf.

Federal Trade Commission (FTC):

- In January 2025, *H&R Block*, a U.S.-based tax-filing service provider, agreed to pay **$7 million** to settle charges that H&R Block unfairly wiped the data that customers who were using H&R Block's online tax-filing service had already entered once the customers chose to downgrade the service they wanted to file their tax returns with.[9]

- In June 2024, the FTC settled charges against *Avast*, a U.K.-based software company, through its Czech subsidiary, alleging that it unfairly collected consumers' browsing information through the company's browser extensions and antivirus software, stored it indefinitely, and sold it without adequate notice and without consumer consent. The FTC also charged that Avast deceived users by claiming that the software would protect consumers' privacy by blocking third party tracking but failed to adequately inform consumers that it would sell their detailed, re-identifiable browsing data. The FTC alleged Avast sold that data to more than 100 third parties through its subsidiary, Jumpshot. The FTC required Avast to pay **$16.5 million** and prohibit the company from selling or licensing any web browsing data for advertising purposes.[10]

- In January of 2024, *Response Tree, LLC*, a U.S.-based lead-generating company, agreed to settle the FTC's charges of consumer privacy breaches for selling the consumer data it obtained through its websites which tricked consumers into providing their personal information, such as their phone numbers, to obtain mortgage services. Response Tree sold this consumer data to telemarketers who used the data to place unrelated telemarketing calls to consumers, including to consumers whose numbers were on the FTC's Do Not Call registry. Response Tree agreed to pay the FTC **$7 million**, was ordered to destroy consumer data obtained prior to January 2024, and was permanently enjoined from collecting or disclosing consumer information arising out of lead generation as well as from initiating or assisting others in initiating similar telemarketing calls.[11]

- In August 2023, *Fluent LLC*, a U.S.-based lead-generating company which operates a "consent farm" enterprise, agreed to pay **$2.5 million** to settle charges that it posted deceptive ads promising monetary rewards and prizes which misled consumers into providing their personal information, including their phone numbers, and then sold consumer information to telemarketing companies without the consumers' consents in violation of the FTC Act. The

[9] *See* FTC, https://www.ftc.gov/legal-library/browse/cases-proceedings/hr-block-matter (enforcement order issued Jan. 07, 2025).
[10] *See* FTC, https://www.ftc.gov/legal-library/browse/cases-proceedings/2023033-avast (enforcement order finalized on Jun. 24, 2024).
[11] *See* FTC, https://www.ftc.gov/legal-library/browse/cases-proceedings/2123087-response-tree-llc (enforcement action filed on Jan. 02, 2024).

telemarketers in turn placed robocalls to consumers using the provided information, including to consumers whose phone numbers were on the Do Not Call registry. In addition to paying the settlement, Fluent was required to implement procedures by which it ensured ads Fluent displayed were not similarly deceptive. Fluent was also permanently enjoined from assisting others in initiating similar robocalls.[12]

- In June 2023, *Publishers Clearing House, LLC (PCH*), a U.S.-based company which organizes sweepstakes and prize-based contests and games, agreed to pay the FTC **$18.5 million** to settle charges that PCH had shared consumers' personal information with third parties in violation of its privacy policy representing PCH would not rent, license, or sell consumer data to any third parties. PCH sold consumer data to third parties which used the data to target consumers using personalized ads on PCH's websites and on other third parties' websites. In addition to the payment, PCH agreed to delete all consumer data that it had collected up until January 2019, which is when PCH removed the portion of its privacy policy stating it did not share consumer data.[13]

- In June 2023, *Microsoft* agreed to pay the FTC **$20 million** to settle charges that Microsoft violated COPPA through its Xbox live gaming platform by collecting and retaining personal data from children without first disclosing to their parents that Microsoft would be collecting the data. Microsoft collected and retained data such as images of the children, their first and last names, and voice and video recordings. Microsoft also agreed to implement a procedure through which Xbox live users were clearly notified of the steps to create a child account which had adequate parental controls and disclosures.[14]

- In May 2022, the FTC finalized charges against *Everalbum, Inc*., a U.S.-based corporation which operates a digital photograph storage application, for violating the FTC Act when Everalbum created datasets based on the photos that users uploaded to the application to improve its facial recognition technology without first obtaining express user consent or first disclosing to users that their photos would be used for this purpose. The FTC also charged Everalbum for falsely representing that it would delete users' photos and videos upon account deactivation. Everalbum was enjoined from making similar future misrepresentations, and was ordered both to obtain affirmative, express user

[12] *See* FTC, https://www.ftc.gov/legal-library/browse/cases-proceedings/1923230-fluent-llc-us-v (enforcement order jointly entered into filed on Aug. 10, 2023).
[13] *See* FTC, https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3145-publishers-clearing-house-llc-pch-ftc-v (enforcement action filed on Jun. 06, 2023).
[14] *See* FTC, https://www.ftc.gov/legal-library/browse/cases-proceedings/1923258-microsoft-corporation-us-v (enforcement order filed on Jun. 09, 2023).

consent before similarly utilizing users' data and to delete all data of users who had deactivated their accounts.[15]

- In January 2022, *ITMedia Solutions LLC*, a lead-generation company, settled charges that it violated Section 5(a) of the FTC Act when it misled consumers into providing sensitive information such as their banking information and Social Security numbers by falsely promising to connect consumers with loan lenders and when it sold consumers' information to third parties without regard for how the information would be used. ITMedia Solutions was ordered to pay **$1.5 million**, was enjoined from selling, transferring, and/or disclosing sensitive consumer information without consumer consent, and was required to improve its recordkeeping over sales, transfers, and/or disclosures of sensitive consumer information where they had consumer consent.[16]

- In June 2021, the FTC finalized charges against *Flo Health, Inc*., a company which operates a woman's health mobile application, for sharing user health information with third parties in violation of its privacy policy stating it would keep such information private. Flo was ordered to instruct such third parties to destroy the shared information, to make clear disclosures to users regarding the ways in which Flo would be using user data, and to obtain a compliance review of their user data privacy practices by a third-party independent assessor. Flo was also prohibited from making similar future misrepresentations regarding its data privacy practices.[17]

- In March 2021, Tapjoy, Inc., a U.S.-based corporation which operates a mobile application advertising platform, settled charges with the FTC for enticing consumers into providing their personal information or into making monetary payments in exchange for virtual currency and other in-app rewards which Tapjoy would either never issue or would issue only after substantial delay. Tapjoy agreed to refrain from engaging in similar practices in the future, to submit a report on its compliance with the order, to implement certain recordkeeping practices moving forward, and to implement additional compliance monitoring procedures.[18]

- In October 2020, the FTC finalized its charges against *NTT Global Data Centers Americas, Inc*. for falsely representing to consumers that it participated in the

[15] *See* FTC, https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3172-everalbum-inc-matter (decision issued on May 6, 2022).
[16] *See* FTC, https://www.ftc.gov/legal-library/browse/cases-proceedings/1523225-itmedia-solutions-llc (enforcement order filed on Jan. 6, 2022).
[17] *See* FTC, https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc (decision and enforcement order finalized on Jun. 22, 2021).
[18] *See* FTC, https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3092-tapjoy-inc-matter (enforcement order issued on Mar. 9, 2021).

Privacy Shield framework and that it was compliant with the framework's privacy requirements. NTT Global was prohibited from making similar future misrepresentations, and was required to meet Privacy Shield requirements, to obtain outside compliance reviews, to implement additional recordkeeping procedures, and to file a compliance report with the FTC.[19]

- In December 2016, the operators of an online dating service agreed to settle Federal Trade Commission and state charges of consumer privacy breaches for failing to protect 36 million users' account and profile information. In addition to a **$1.6 million** penalty, the company was required to implement a comprehensive data security program, which includes third-party assessments.

- In February 2016, a multinational computer hardware company agreed to settle FTC charges that its routers contained critical security flaws that put consumers' home networks at risk. As part of the settlement, the company was required to implement a comprehensive security program and will be subject to independent audits for the next **20 years** following the settlement.[20]

- In January of 2016, a provider of office management software for dental practices agreed to pay **$250,000** to settle FTC charges that it had falsely advertised the level of encryption it provided to protect patient data.[21]

- In December 2015, the FTC entered into a settlement with an ID protection services company requiring the company to pay **$100 million** to settle contempt charges that it had violated the terms of a 2010 federal court order requiring the company to secure consumers' personal information and prohibiting deceptive advertising.[22]

- In December 2015, two app developers agreed to pay a combined **$360,000** in penalties to settle charges that they had violated COPPA. According to the complaint, the developers had created a number of apps targeted at children and allowed third-party advertisers to collect the children's personal information through the apps. The complaints against the developers alleged that they did

[19] *See* FTC, https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3189-ntt-global-data-centers-americas-inc-matter (enforcement order issued on Oct. 28, 2020).
[20] https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.
[21] https://www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled.
[22] https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated.

not provide notice or get consent from children's parents for collecting and using the information.[23]

- In December 2015, the FTC settled charges that a hotel and resort chain had unfairly exposed the payment card information of consumers to hackers through three separate data breaches. Under the settlement, the terms of which are in place for 20 years, the company was required to implement a comprehensive information security program and to obtain an annual security audit. The company is also required to obtain an assessment in the event of a breach of more than 10,000 payment card numbers and provide that assessment to the FTC within 10 days.[24]

Securities and Exchange Commission:

- In January 2025, twelve firms agreed to pay the SEC more than **$63 million** to settle charges for recordkeeping failures associated with federal securities laws. Nine investment advisors and three broker-dealers were charged with failing to maintain and preserve electronic communications.[25]

- In December 2024, the SEC announced that it ordered *Flagstar Bancorp* to pay a **$3.55 million** civil penalty to the SEC for its failure to protect sensitive customer data which led to a data breach and an exfiltration of the personally identifiable information of about 1.5 million people in violation of both the Securities Act of 1933 and the Securities Exchange Act of 1934.[26]

- In October 2024, the SEC announced it charged four public companies, *Unisys Corp., Avaya Holdings Corp., Check Point Software Technologies Ltd, and Mimecast Limited*, with making materially misleading disclosures regarding their cybersecurity risks and processes in violation of the Securities Act, the Securities Exchange Act, and related SEC rules. Specifically, the companies failed to disclose material information regarding their risk of cyberattack. The SEC ordered the companies to pay a total of approximately **$7 million** to settle the charges. Unisys was ordered to pay **$4 million**; Avaya was ordered to pay **$1 million**,

[23] https://www.ftc.gov/news-events/press-releases/2015/12/two-app-developers-settle-ftc-charges-they-violated-childrens.
[24] https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.
[25] *See* SEC, https://www.sec.gov/newsroom/press-releases/2025-6 (press release dated Jan. 13, 2025).
[26] *See* SEC, https://www.sec.gov/enforcement-litigation/administrative-proceedings/33-11343-s (press release dated Dec. 16, 2024).

Check Point was ordered to pay **$995,000**, and Mimecast was ordered to pay **$990,000**.[27]

- In October 2023, the SEC announced it brought charges against SolarWinds, a United States-based software company, for fraud and internal control failures relating to its cybersecurity risks and vulnerabilities in violation of the Securities Act, the Securities Exchange Act, and related SEC rules. Specifically, the SEC alleged SolarWinds defrauded investors by overstating its cybersecurity practices and either understating or failing to disclose allegedly known cybersecurity risks in its filings to the SEC.[28]

- In March 2023, the SEC announced that it settled charges against *Blackbaud Inc.*, a United States-based data management software company, for making misleading disclosures about a ransomware attack that compromised sensitive customer information and affected more than 13,000 customers. Blackbaud agreed to pay the SEC **$3 million** as part of the settlement.[29]

- In June 2016, *Morgan Stanley* agreed to pay a **$1 million** penalty to settle charges brought by the Securities and Exchange Commission. The charges related to the bank's failure to protect customer information, some of which were hacked by a former employee and offered for sale online, and inadequate written consumer data policies.[30]

- In September 2015, *R.T. Jones*, an investment advisor, paid **$75,000** to settle charges that it failed to establish the required cybersecurity policies and procedures. After a breach compromised the personally-identifiable information (PII) of approximately 100,000 individuals, the firm promptly notified potential victims and offered free identity theft monitoring.[31]

U.S. Department of Health and Human Services (HHS):

- In August 2025, HHS announced a **$175,000** settlement with BST & Co. CPAs, LLP for a HIPAA Security Rule violation resulting from a 2019 ransomware attack. In

[27] *See* SEC, https://www.sec.gov/newsroom/press-releases/2024-174 (press release dated Oct. 22, 2024); *see also* SEC, *Statement Regarding Administrative Proceedings Against SolarWinds Customers*, https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-solarwinds-102224 (statement dated Oct. 22, 2024).
[28] *See* SEC, https:/www.sec.gov/enforcement-litigation/litigation-releases/lr-25887 (press release dated Oct. 31, 2023).
[29] *See* SEC, https://www.sec.gov/newsroom/press-releases/2023-48 (press release dated Mar. 9, 2023).
[30] *See* SEC Press Release, https://www.sec.gov/news/pressrelease/2016-112.html.
[31] *See* SEC Press Release, https://www.sec.gov/news/pressrelease/2015-202.html.

addition to paying the settlement amount, the company was also ordered to implement a two-year corrective action plan to improve its security measures.[32]

- In April 2025, *Syracuse ASC, LLC*, a U.S.-based specialty surgery practice, settled charges alleging it HIPAA when it failed to conduct an accurate and thorough HIPAA security risk analysis over its network storing electronic protected health information (hereinafter ePHI). Syracuse's failure allegedly allowed a threat actor to gain access to Syracuse's network for more than two weeks. The breach affected upwards of 24,000 individuals who were current and former patients of the practice; the ePHI affected included names, dates of birth, Social Security numbers, financial information, and clinical treatment information. Syracuse agreed to pay **$250,000** to settle charges.[33]

- In February 2025, *Cornstar LLC*, a U.S.-based medical billing company, settled charges alleging it had violated HIPAA when it failed to maintain accurate and thorough network server vulnerability and risk management assessments. Cornstar's failure allowed an unknown party to gain access to the protected health information (hereinafter PHI) of 585,621 users that *Cornstar* held on its servers. As part of its agreement with the HHS to settle charges, *Cornstar* agreed to pay the HHS a **$75,000** penalty and agreed to implement a corrective action plan.[34]

- In February 2025, *BayCare Health System*, a U.S.-based hospital network which operates hospitals in Florida, settled HHS charges that alleged it violated HIPAA when its failure to conduct compliance reviews and implement procedures safeguarding a patient's medical information allowed an unknown and unauthorized third-party to access the information. As part of its agreement with the HHS to settle charges, *BayCare* agreed to pay an **$800,000** penalty and agreed to implement a corrective action plan.[35]

- In February 2025, *Vision Upright MRI LLC*, a U.S.-based medical imaging provider, agreed to settle HHS charges alleging it violated HIPAA when it failed to conduct a risk analysis over its communications system which stored medical images (e.g., MRI, CT, and x-ray scans) and when it failed to timely notify individuals affected by a breach of its system. Vision Upright agreed to pay a **$25,000**

[32] *See* HHS (https://www.hhs.gov/sites/default/files/hhs-ocr-bst-hipaa-settlement.pdf) (press release dated Aug. 18, 2025).
[33] *See HHS* (https://www.hhs.gov/sites/default/files/ocr-hipaa-racap-syracuse-asc.pdf) (agreement signed Apr. 2, 2025).
[34] *See* HHS (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/hhs-hipaa-agreement-comstar/index.html) (agreement signed on Feb. 19, 2025).
[35] *See* HHS (https://www.hhs.gov/sites/default/files/hhs-ocr-hipaa-baycare-agreement.pdf) (agreement signed on Feb. 14, 2025).

penalty and agreed to implement a corrective action plan to settle the HHS charges.[36]

- In February 2025, *Comprehensive Neurology, PC*, a U.S.-based medical clinic owned by a single medical practitioner, agreed to settle charges that it violated HIPAA when it failed to perform risk assessments over its electronic protected health information (hereinafter ePHI) storage system, allowing it to be vulnerable to a ransomware attack which may have affected the medical records of up to 6,800 patients. Comprehensive Neurology agreed to pay a **$25,000** penalty and agreed to implement a corrective action plan to settle the charges.[37]

- In February 2025, *Guam Memorial Hospital Authority* settled HHS charges alleging the Authority violated HIPAA. After finding out the Authority was subject to a ransomware attack which affected the stored health information of about 5,000 individuals and finding former employees were able to access the information system, HHS charged the Authority for a failure to conduct risk and vulnerability assessments over its health information storage system. The Authority agreed to pay a **$25,000** penalty and implement a corrective action plan to settle the charges.[38]

- In January 2025, *PIH Health, Inc*., a U.S.-based regional healthcare network, agreed to pay a **$600,000** penalty and implement a corrective action plan to settle charges that it violated the HHS when it failed to conduct risk analyses over its system storing medical information and when it failed to timely notify affected individuals, the media, and the HHS Secretary of a data breach exposing the medical information of 189,763 individuals.[39]

- In January 2025, HHS announced a settlement with *South Broward Hospital District*, operating as Memorial Healthcare System, for a potential violation of HIPAA's Privacy Rule regarding timely access to protected health information (PHI). The settlement resolves a complaint alleging that Memorial Healthcare System did not provide timely access to an individual's medical records. Following an investigation, OCR found that the health system failed to respond within the required 30 days. Memorial Healthcare System has agreed to pay **$60,000**, marking OCR's 52nd Right of Access enforcement action. The individual

[36] *See* HHS (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/hhs-ocr-hipaa-racap-vum/index.html) (agreement signed on Feb. 12, 2025).
[37] *See* HHS (https://www.hhs.gov/sites/default/files/ocr-hipaa-racap-np.pdf) (agreement signed on Feb. 10, 2025).
[38] *See* HHS (https://www.hhs.gov/sites/default/files/ocr-hipaa-recap-gmha.pdf) (agreement signed on Feb. 06, 2025).
[39] *See* HHS (https://www.hhs.gov/sites/default/files/ocr-hipaa-racap-pih.pdf) (agreement signed on Jan. 28, 2025).

did not receive access to their records until approximately nine months after the initial request.[40]

- In January 2025, HHS announced a settlement with *Solara Medical Supplies, LLC*, for potential violations of the HIPAA Security Rule and Breach Notification Rule following a phishing incident that compromised electronic protected health information (ePHI) of 114,007 individuals. The investigation revealed that Solara failed to conduct a compliant risk analysis, implement adequate security measures, and provide timely breach notifications. Under the resolution agreement, Solara will pay **$3 million** and implement a corrective action plan monitored by OCR for two years, which includes conducting a thorough risk analysis, developing a risk management plan, revising policies, and training its workforce on HIPAA compliance.[41]

- In January 2025, HHS announced a **$90,000** settlement with *Virtual Private Network Solutions, LLC* (VPN Solutions) for a potential violation of the HIPAA Security Rule following a ransomware attack on its information system. The investigation revealed that VPN Solutions failed to conduct a compliant risk analysis to identify vulnerabilities in its electronic protected health information (ePHI) systems. The ransomware incident, reported in December 2021, affected twelve covered entities and compromised sensitive data, including personal identifiers and health information. Under the settlement, VPN Solutions will implement a corrective action plan and be monitored by OCR for one year to ensure compliance with HIPAA.[42]

- In January 2025, HHS announced an **$80,000** settlement with *Elgon Information Systems* for potential violations of the HIPAA Security Rule following a ransomware attack on its information system. The investigation revealed that Elgon failed to conduct a thorough risk analysis, which allowed an unauthorized actor to access its server, affecting approximately 31,248 individuals' electronic protected health information (ePHI). Under the settlement, Elgon will implement a corrective action plan, which includes updating its risk analysis, enhancing its risk management plan, revising policies, and providing workforce training on HIPAA compliance. HHS will monitor Elgon for three years to ensure compliance.[43]

[40] https://www.hhs.gov/about/news/2025/01/15/hhs-office-civil-rights-settles-hipaa-case-against-memorial-healthcare-system-over-patient-access-records.html (press release dated Jan. 15, 2025).
[41] *See* HHS (https://www.hhs.gov/about/news/2025/01/14/hhs-office-civil-rights-settles-hipaa-phishing-cybersecurity-investigation-solara-medical-supplies-3000000.html) (press release dated Jan. 14, 2025).
[42] *See* HHS (https://www.hhs.gov/about/news/2025/01/07/hhs-office-civil-rights-settles-9th-ransomware-investigation-virtual-private-network-solutions.html) (press release dated Jan. 7, 2025).
[43] *See* HHS (https://www.hhs.gov/about/news/2025/01/07/hhs-office-civil-rights-settles-8th-ransomware-investigation-elgon-information-systems.html) (press release dated Jan. 7, 2025).

- In December 2024, *Northeast Radiology, P.C.* agreed to pay the HHS a **$350,000** penalty and agreed to implement a corrective action plan after the HHS charged Northeast with violating HIPAA. The HHS alleged Northeast's failure to perform risk and vulnerability assessments over its radiology image storage system may have led to a breach which allowed unauthorized parties to access patient radiology images.[44]

- In December 2024, *Health Fitness Corporation* reached a Resolution Agreement with the HHS to settle allegations of HIPAA violations. The issues arose from a software misconfiguration that exposed ePHI on the internet. Health Fitness did not discover the exposure until approximately three years later. HHS alleged the exposure, and Health Fitness's failure to detect it, was caused by Health Fitness's failure to conduct thorough risk and vulnerability assessments. As part of the settlement, Health Fitness agreed to pay the HHS **$227,816** and comply with a corrective action plan.[45]

- In December 2024, HHS settled a **$200,000** penalty against *Oregon Health & Science University (OHSU)* for violating an individual's right to timely access medical records. Under HIPAA's Privacy Rule, covered entities must provide access to health information within 30 days of a request. OCR's investigation followed a complaint from January 2021, revealing that OHSU failed to provide all requested records until August 2021—delaying access to medical records for over a year.[46]

- In December 2024, HHS imposed a **$1.5 million** civil money penalty on *Warby Parker, Inc*. for violations of the HIPAA Security Rule following a breach report regarding unauthorized access to customer accounts. The breach involved unauthorized third parties accessing 197,986 customer accounts through "credential stuffing," exposing ePHI such as names, addresses, and payment information. HHS found Warby Parker failed to conduct a thorough risk analysis, implement adequate security measures, and regularly review system activity.[47]

- In December 2024, HHS settled with *South Broward Hospital District*, operating as Memorial Healthcare System, for a potential violation of HIPAA's Privacy Rule regarding timely access to protected health information (PHI). The settlement resolves a complaint alleging that Memorial Healthcare System did not provide

[44] *See* HHS (https://www.hhs.gov/sites/default/files/ocr-hipaa-settlement-nerad.pdf) (agreement signed on Dec. 27, 2024).
[45] *See* HHS (https://www.hhs.gov/sites/default/files/ocr-health-fitness-ra-cap.pdf) (agreement signed on Dec. 20, 2024).
[46] *See* HHS (https://www.hhs.gov/press-room/penalty-against-or-health-science-university.html) (agreement signed on Dec. 13, 2024).
[47] *See* HHS (https://www.hhs.gov/sites/default/files/ocr-warby-parker-nfd.pdf) (notice of final determination dated Dec. 11, 2024).

timely access to an individual's medical records. Following an investigation, OCR found that the health system failed to respond to an individual's request for medical information within the required 30 days. The individual did not receive access to their records until approximately nine months after the initial request. Memorial Healthcare System has agreed to pay **$60,000**.[48]

- In December 2024, HHS announced a settlement with *Inmediata Health Group, LLC*, for potential violations of the HIPAA Security Rule after a complaint revealed that protected health information (PHI) was accessible online via search engines. From May 2016 to January 2019, the PHI of 1,565,338 individuals, including names, Social Security numbers, and medical information, was publicly available. OCR's investigation identified failures in conducting a compliant risk analysis and monitoring health information systems. Inmediata agreed to pay **$250,000** to resolve the investigation, and no additional corrective action plan was required as Inmediata had previously settled with 33 states on related issues.[49]

- In December 2024, HHS announced a civil monetary penalty of **$548,265** against *Children's Hospital Colorado* for violations of the HIPAA Privacy and Security Rules following breach reports related to email phishing and cyberattacks in 2017 and 2020. The breaches compromised the protected health information (PHI) of 3,370 and 10,840 individuals, respectively. Investigations revealed that multi-factor authentication was disabled on an email account and that workforce members granted access to unknown third parties. Additionally, the hospital failed to train staff on HIPAA requirements and conduct a compliant risk analysis. Children's Hospital Colorado waived its right to a hearing, leading to the imposition of the penalty.[50]

- In December 2024, HHS announced a civil monetary penalty of **$1.19 million** against *Gulf Coast Pain Consultants, LLC*, for violations of the HIPAA Security Rule following a breach report that revealed a former contractor improperly accessed the electronic medical record system. This unauthorized access affected approximately 34,310 individuals, compromising sensitive information such as names, Social Security numbers, and insurance details. OCR identified four violations, including failures to conduct a proper risk analysis and to terminate

[48] *See* HHS (https://www.hhs.gov/about/news/2025/01/15/hhs-office-civil-rights-settles-hipaa-case-against-memorial-healthcare-system-over-patient-access-records.html) (settlement agreement dated Dec. 11, 2024).
[49] *See* HHS (https://www.hhs.gov/about/news/2024/12/10/hhs-office-civil-rights-settles-health-care-clearinghouse-inmediata-health-group-hipaa-impermissible-disclosure.html) (Dec. 10, 2024).
[50] (https://www.hhs.gov/about/news/2024/12/05/hhs-ocr-imposes-548-265-penalty-against-childrens-hospital-colorado-hipaa-privacy-security-rules-violations.html) (Dec. 5, 2024).

access for former workforce members. Gulf Coast waived its right to a hearing, resulting in the imposition of the penalty.[51]

- In November 2024, HHS announced a settlement with *Holy Redeemer Family Medicine*, a U.S.-based hospital, for an alleged violation of the HIPAA Privacy Rule due to the impermissible disclosure of a female patient's protected health information, including sensitive reproductive health details, to her prospective employer. OCR's investigation revealed that Holy Redeemer disclosed the patient's full medical record without her authorization and without any applicable exception under the Privacy Rule. As part of the resolution, Holy Redeemer paid **$35,581** and agreed to implement a corrective action plan, which includes revising policies, training staff, and submitting compliance reports to OCR over the next two years.[52]

- In November 2024, HHS announced a **$100,000** penalty against U.S.-based Rio Hondo Community Mental Health Center for failing to provide a patient with timely access to their medical records. The investigation was initiated after a patient complained about not receiving their records despite multiple requests over nearly seven months. OCR found that Rio Hondo did not act promptly to fulfill the patient's right of access. Rio Hondo waived its right to a hearing and did not contest the findings, resulting in the imposition of the penalty.[53]

- In November 2024, HHS entered into a resolution agreement with *Northeast Surgical Group, P.C. (NESG)* following a ransomware breach affecting approximately 15,298 individuals. HHS's investigation revealed that NESG failed to conduct a thorough risk assessment of its electronic protected health information (ePHI). As part of the settlement, NESG agreed to pay a **$10,000** resolution amount and comply with a Corrective Action Plan.[54]

- In October 2024, HHS announced a settlement with Bryan County Ambulance Authority, a U.S.-based emergency medical service provider, for a potential violation of the HIPAA Security Rule following a ransomware attack on its information systems. The incident affected the protected health information of 14,273 patients. OCR's investigation revealed that BCAA failed to conduct a compliant risk analysis to identify vulnerabilities in its systems. BCAA agreed to pay **$90,000** and implement a corrective action plan, which includes conducting

[51] (https://www.hhs.gov/about/news/2024/12/03/hhs-ocr-imposes-penalty-against-gulf-coast-pain-consultants.html) (Dec. 3, 2024).
[52] (https://www.hhs.gov/about/news/2024/11/26/hhs-office-civil-rights-settles-holy-redeemer-hospital-disclosure-patients-protected-health-information-including-reproductive-health-information.html) (Nov. 26, 2024).
[53] https://www.hhs.gov/about/news/2024/11/19/hhs-office-civil-rights-imposes-penalty-mental-health-center-failure-provide-timely-access-patient-records.html (Nov. 19, 2024).
[54] *See* HHS (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/northeast-surgical-group-ra-cap/index.html) (resolution agreement signed Nov. 14, 2024).

a thorough risk analysis, developing a risk management plan, and training its workforce on HIPAA compliance.[55]

- In October 2024, HHS announced a **$500,000** settlement with *Plastic Surgery Associates of South Dakota* for potential violations of the HIPAA Security Rule following a ransomware attack that compromised the PHI of 10,229 individuals. The investigation revealed that the attack stemmed from a brute force method used to access the network, and the organization failed to conduct a compliant risk analysis and implement adequate security measures. As part of the settlement, Plastic Surgery Associates agreed to a corrective action plan that includes conducting a thorough risk analysis, implementing security policies, and providing workforce training on HIPAA compliance.[56]

- In October 2024, HHS announced a **$70,000** civil monetary penalty against *Gums Dental Care, LLC*, for failing to provide timely access to a patient's medical records, as required by the HIPAA Privacy Rule. Gums Dental Care challenged the penalty, but the decision was upheld by an Administrative Law Judge and later affirmed by the Departmental Appeals Board.[57]

- In October 2024, HHS announced a **$240,000** civil monetary penalty against Providence Medical Institute for potential violations of the HIPAA Security Rule following a ransomware attack that impacted the ePHI of 85,000 individuals in early 2018. The investigation revealed that the institute did not implement adequate policies to restrict access to ePHI. Providence Medical Institute waived its right to a hearing and did not contest the findings, resulting in the penalty.[58]

- In September 2024, HHS announced a **$250,000** settlement with *Cascade Eye and Skin Centers* for potential violations of the HIPAA Security Rule following a ransomware attack that affected approximately 291,000 files containing ePHI. The investigation revealed that the center failed to conduct a compliant risk analysis and did not adequately monitor its health information systems to prevent cyberattacks. As part of the settlement, Cascade Eye and Skin Centers will implement a corrective action plan, which includes conducting a thorough

[55] *See* HHS (https://www.hhs.gov/about/news/2024/10/31/hhs-office-for-civil-rights-settles-hipaa-ransomware-cybersecurity-investigation-for-90000-dollars.html) (Oct. 31, 2024).
[56] *See* HHS (https://www.hhs.gov/about/news/2024/10/31/hhs-office-civil-rights-settles-ransomware-cybersecurity-investigation-500000.html) (Oct. 31, 2024).
[57] *See* HHS (https://www.hhs.gov/about/news/2024/10/17/hhs-office-civil-rights-imposes-70000-civil-monetary-penalty-against-gums-dental-care-failure-provide-timely-access-patient-records.html) (Oct. 17, 2024).
[58] (https://www.hhs.gov/about/news/2024/10/03/hhs-ocr-imposes-civil-monetary-penalty-against-providence-medical-institute-hipaa-ransomware-cybersecurity-investigation.html) (Oct. 3, 2024).

risk analysis, developing security policies, and ensuring regular reviews of system activity.[59]

- In July 2024, HHS announced a **$950,000** settlement with *Heritage Valley Health System* for potential violations of the HIPAA Security Rule following a ransomware attack. The investigation revealed multiple violations, including failure to conduct a compliant risk analysis, implement a contingency plan for emergencies, and restrict access to ePHI. As part of the settlement, Heritage Valley will implement a corrective action plan monitored by OCR for three years, which includes conducting a thorough risk analysis, developing a risk management plan, and training staff on HIPAA compliance. OCR emphasized the importance of safeguarding patient information to prevent cyberattacks.[60]

- In January 2024, HHS's Office for Civil Rights (OCR) finalized a civil monetary penalty of **$100,000** against Essex Residential Care LLC, a nursing care facility doing business as Hackensack Meridian Health, West Caldwell Care Center (WCCC), for violations of the HIPAA Privacy Rule. The penalty stems from WCCC's failure to provide timely access to a patient's medical records. WCCC waived its right to a hearing and did not contest the findings, resulting in the penalty being imposed.[61]

- In November 2023, *Montefiore Medical Center* entered into a Settlement Agreement with HHS's Office for Civil Rights (OCR) to resolve potential violations of the HIPAA Security Rule following a breach of its unsecured ePHI. The Medical Center discovered that one of its employees accessed the ePHI of 12,517 patients and sold some of that information to an identity theft ring. The Medical Center was required to pay **$4.75 million** and implement a corrective action plan to ensure compliance with HIPAA requirements. This plan includes conducting a comprehensive risk analysis, developing a risk management plan, and training staff in HIPAA policies. OCR will monitor compliance for two years.[62]

- In October 2023, the HHS charged *Doctors' Management Services, Inc*. (DMS) with violating HIPAA after a ransomware attack exposed the protected health information of approximately 206,695 individuals. DMS agreed to pay **$100,000** and comply with a Corrective Action Plan to address the violations, which

[59] (https://www.hhs.gov/about/news/2024/09/26/hhs-office-civil-rights-settles-ransomware-cybersecurity-investigation-under-hipaa-security-rule-250-000.html) (Sep. 26, 2024).
[60] (https://www.hhs.gov/about/news/2024/07/01/hhs-office-civil-rights-settles-hipaa-security-rule-failures-950000.html) (Jul. 1, 2024).
[61] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/hackensack-meridian-health-west-caldwell-care-center/index.html#nfd) (notice of final determination dated Apr. 1, 2024).
[62] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/montiefore/index.html) (resolution agreement signed Nov. 17, 2023).

included failing to conduct a thorough risk analysis and implement necessary security measures.[63]

- In October 2023, the HHS charged *Green Ridge Behavioral Health, LLC* (GRBH) with violating HIPAA following a ransomware attack that compromised the protected health information of over 14,000 patients. GRBH agreed to pay **$40,000** and comply with a Corrective Action Plan to address its noncompliance, which included failures in risk analysis, security measures, and proper handling of protected health information.[64]

- In November 2023, *Optum Medical Care*, a private multi-specialty physician group, entered into a Resolution Agreement with HHS's Office for Civil Rights (OCR) to address potential violations of the HIPAA Privacy Rule for its failure to provide patient medical information. The agreement outlines that Optum will pay a civil monetary penalty of **$160,000** and implement a corrective action plan (CAP) to enhance compliance with HIPAA requirements.[65]

- In August 2023, the HHS charged a New Jersey-based hospital with violating HIPAA's Privacy rule and ordered it to pay **$80,000** for allowing a reporter to observe COVID-19 patients and access the protected health information of COVID-19 patients without proper authorization. Hospital also agreed to enter into and comply with a Corrective Action Plan.

- In August 2023, the HHS entered into a Resolution Agreement with *UnitedHealthcare Insurance Company* (UHIC) after an investigation revealed that, in violation of HIPAA's right of access provisions, UHIC failed to timely provide a member access to their medical records due to employee error. UHIC agreed to pay **$80,000** and comply with a Corrective Action Plan to address the violation.[66]

- In August 2023, the HHS charged *L.A. Care Health Plan* (LACHP) with violating HIPAA after incidents in 2014 and 2019 allowed members to view each other's protected health information due to processing errors. LACHP agreed to pay **$1.3 million** and comply with a Corrective Action Plan to address its noncompliance,

[63] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/dms-ra-cap/index.html) (press release dated Oct. 31, 2023).
[64] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/green-ridge-behavioral-health-ra-cap/index.html) (resolution agreement signed Oct. 31, 2023).
[65] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/optum-medical-care.html) (press release dated Nov. 15, 2023).
[66] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/uhc-ra-cap/index.html) (resolution agreement signed Aug. 8, 2023).

which included failures in risk analysis, security measures, and proper handling of protected health information.[67]

- In May 2023, the HHS entered into a Resolution Agreement with *Yakima Valley Memorial Hospital* after an investigation into a data breach incident revealed potential violations of HIPAA's Security Rule. Yakima agreed to pay **$240,000** and comply with a Corrective Action Plan to rectify the violations.[68]

- In April 2023, the HHS entered into a Resolution Agreement with *iHealth Solutions, LLC*, after a breach report revealed that the ePHI of 267 individuals was exfiltrated from an insecure server by an unauthorized party. iHealth agreed to pay **$75,000** and comply with a Corrective Action Plan to address violations of HIPAA regulations, including failures in risk assessment and unauthorized disclosure of protected health information.[69]

- In March 2023, *Manasa Health Center LLC*, a medical practice, agreed to pay **$30,000** to settle HHS charges that it violated HIPAA when it responded to the negative reviews that patients posted online about the practice by disclosing patient PHI.[70]

- In March 2023, the HHS entered into a Resolution Agreement with *MedEvolve, Inc*., a medical software service provider, after a breach report revealed that the PHI of 230,572 individuals was accessible on the internet due to an unsecured File Transfer Protocol (FTP) server. *MedEvolve* agreed to pay **$350,000** and comply with a Corrective Action Plan to address violations of HIPAA regulations, including failures in risk assessment and the lack of a business associate agreement with a subcontractor.[71]

- In January 2023, the HHS entered into a Resolution Agreement with *David Mente, MA, LPC*, after an investigation found that he failed to provide a parent with timely access to his minor child's PHI as required by HIPAA. David Mente

[67] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/la-care-health-plan/index.html) (resolution agreement signed Aug. 1, 2023).
[68] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/yakima-ra-cap/index.html) (resolution agreement signed May 15, 2023).
[69] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ihealth-ra-cap/index.html) (resolution agreement signed Apr. 20, 2023).
[70] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/manasa-ra-cap/index.html) (resolution agreement signed Mar. 28, 2023).
[71] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/medevolve-ra-cap/index.html) (resolution agreement signed Mar. 17, 2023).

agreed to pay **$15,000** and comply with a Corrective Action Plan to address the violations related to the Privacy Rule.[72]

- In December 2022, the HHS entered into a Resolution Agreement with *Banner Health*, a U.S.-based hospital system, following an investigation into a breach incident where an unauthorized party gained access to the ePHI of approximately 2.81 million individuals through Banner Health's information system. Banner agreed to pay **$1.25 million** and comply with a Corrective Action Plan to address violations of HIPAA regulations, including failures in risk analysis and security measures to protect patient information.[73]
- In December 2022, the HHS entered into a Resolution Agreement with *Life Hope Labs* after a complaint revealed that the organization failed to provide timely access to a patient's medical records, taking 225 days to respond to a request. Life Hope Labs agreed to pay **$16,500** and comply with a Corrective Action Plan to address violations of HIPAA regulations regarding access to protected health information.[74]
- In November 2022, the HHS entered into a Resolution Agreement with *Health Specialists of Central Florida* after an investigation revealed that the organization failed to provide timely access to a deceased patient's medical records. The Covered Entity agreed to pay **$20,000** and comply with a Corrective Action Plan to address violations of HIPAA regulations regarding patient access to protected health information.[75]
- In November 2022, the HHS entered into a Resolution Agreement with *New Vision Dental* after an investigation revealed that the practice impermissibly disclosed PHI on its Yelp business page and failed to implement required privacy practices. New Vision Dental agreed to pay **$23,000** and comply with a Corrective Action Plan to address violations of HIPAA regulations regarding patient privacy and information disclosure.[76]
- In December 2022, the HHS announced it settled the charges it brought against three dental practices for violating HIPAA when each practice failed to provide their patients with timely access to their medical records as part of its Right of

[72] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/mente-ra-cap/index.html) (resolution agreement signed on Jan. 5, 2023).
[73] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/banner-health/index.html) (resolution agreement signed on Dec. 21, 2022).
[74] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/life-hopes-ra-cap/index.html) (resolution agreement signed on Dec. 14, 2022).
[75] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/health-specialists-ra-cap/index.html) (resolution agreement signed on Nov. 15, 2022).
[76] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/new-vision-ra-cap/index.html) (resolution agreement signed on Nov. 14, 2022).

Access initiatives. HHS imposed a monetary penalty on the practices ranging from **$25,000 to $80,000** and ordered each of the practices to implement a corrective plan.[77]

- In July 2022, the HHS entered into a Resolution Agreement with *New England Dermatology* after a breach report revealed that the practice improperly disposed of specimen containers labeled with PHI in a dumpster, compromising patient privacy. New England Dermatology agreed to pay **$300,640** and comply with a Corrective Action Plan to address violations of HIPAA regulations regarding the safeguarding of PHI and disclosure practices.[78]

- In July 2022, the HHS announced it settled the charges it brought against 11 medical practices for violating HIPAA's practices for violating HIPAA when each practice failed to provide their patients with timely access to their medical records as part of its Right of Access initiatives. HHS imposed a monetary penalty on the practices ranging from **$3,500 to $240,000**.[79]

- In May 2022, the HHS entered into a Resolution Agreement with Oklahoma State University – Center for Health Sciences (OSU-CHS) after a breach incident revealed that an unauthorized third party accessed protected health information (PHI) affecting 279,865 individuals. OSU-CHS agreed to pay **$875,000** and comply with a Corrective Action Plan to address violations of HIPAA regulations concerning the safeguarding of PHI and proper breach notification practices.[80]

- In March 2022, the HHS announced it settled the charges it brought against **four** medical practices for violating HIPAA's practices for violating HIPAA when each practice failed to provide their patients with timely access to their medical records as part of its Right of Access initiatives. HHS imposed a monetary penalty on the practices ranging from **$28,000 to $62,500**.[81]

- In November 2021, the HHS announced it settled the charges it brought against **five** medical practices for violating HIPAA's practices for violating HIPAA when each practice failed to provide their patients with timely access to their medical

[77] (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/new-vision-ra-cap/index.html) (press release dated Dec. 14, 2022).
[78] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/nedlc-ra-cap/index.html) (resolution agreement signed on Jul. 26, 2022).
[79] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/july-2022-hipaa-enforcement/index.html) (press release dated Jul. 15, 2022).
[80] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/osu/index.html) (resolution agreement signed on May 10, 2022).
[81] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/july-2022-hipaa-enforcement/index.html) (press release dated Mar. 28, 2022).

records as part of its Right of Access initiatives. HHS imposed a monetary penalty on the practices ranging from **$10,000 to $160,000**.[82]

- In August 2021, the HHS entered into a Resolution Agreement with Children's Hospital & Medical Center (CHMC) after an investigation revealed that the hospital failed to provide timely access to a deceased patient's medical records, taking several months to fulfill the request. CHMC agreed to pay **$80,000** and comply with a Corrective Action Plan to address violations of HIPAA regulations regarding patient access to protected health information.[83]

- In April 2021, the HHS entered into a Resolution Agreement with the Diabetes, Endocrinology & Lipidology Center, Inc. (DELC) after an investigation revealed that DELC failed to provide timely access to a deceased patient's protected health information. DELC agreed to pay **$5,000** and comply with a Corrective Action Plan to address violations of HIPAA regulations regarding patient access to health information.[84].

- In March 2021, the HHS entered into a Resolution Agreement with Village Plastic Surgery (VPS) to settle charges that VPS violated HIPAA when it failed to provide a patient with timely access to their medical records. VPS agreed to pay **$30,000** and comply with a Corrective Action Plan to settle the charges.[85]

- In March 2021, The Arbour, Inc. agreed to pay **$65,000** and agreed to comply with a Corrective Action Plan to settle HHS charges that The Arbour violated HIPAA's right of access standard when it failed to provide a patient with timely access to their medical records.[86]

- In February 2021, Sharp HealthCare agreed to pay **$70,000** and agreed to comply with a Corrective Action Plan to settle HHS charges that it violated HIPAA's right of access standard when it failed to timely respond to a patient's request for their medical records.[87]

---

[82] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/2021-right-of-access-initiative/index.html) (press release dated Nov. 30, 2021).
[83] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/chmc/index.html) (resolution agreement signed on Aug. 17, 2021).
[84] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/delc/index.html) (resolution agreement signed on Apr. 28, 2021).
[85] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/vps/index.html) (resolution agreement signed on Mar. 8, 2021).
[86] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/arbour/index.html) (resolution agreement signed on Mar. 9, 2021).
[87] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/sharp/index.html) (resolution agreement signed on Feb. 03, 2021).

- In February 2021, Renown Health P.C. agreed to pay **$75,000** and agreed to comply with a Corrective Action Plan to settle HHS charges that it violated HIPAA's right of access standard when it failed to timely respond to a patient's request for their medical records.[88]

- In January 2021, Excellus Health Plan, Inc. agreed to pay **$5.1 million** and agreed to comply with a Corrective Action Plan to settle HHS charges that Excellus violated HIPAA's Privacy, Security, and Breach Notification Rules. The HHS found Excellus violated these HIPAA rules when HHS received a report that cyberattackers gained unauthorized access to Excellus's IT systems which included the ePHI of about 10 million people. The HHS found Excellus failed to conduct risk analyses over its IT system, failed to implement cyber security measures to reduce the risk that the ePHI stored on its system would be compromised, failed to regularly review its IT system activity, and failed to prevent unauthorized access to its IT system in violation of HIPAA.[89]

- In January 2021, Banner Health agreed to pay **$200,000** and agreed to comply with a Corrective Action Plan to settle HHS charges that it violated HIPAA's right of access standard when it failed to timely respond to a patient's request for their medical records.[90]

- In December 2020, Peter Wrobel, M.D., P.C. agreed to pay **$36,000** and agreed to comply with a Corrective Action Plan to settle HHS charges that it violated HIPAA's right of access standard when it failed to timely respond to a patient's request for their medical records.[91]

- In November 2020, The University of Cincinnati Medical Center, LLC agreed to pay **$65,000** and agreed to comply with a Corrective Action Plan to settle HHS charges that it violated HIPAA's right of access standard when it failed to timely respond to a patient's request for their medical records.[92]

- In October 2020, the HHS entered into a Resolution Agreement with Dr. Rajendra Bhayani, a private practitioner, after an investigation revealed that Dr. Bhayani failed to provide a patient with timely access to their medical records at

[88] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/renown/index.html) (resolution agreement signed on Feb. 02, 2021).
[89] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/excellus/index.html) (resolution agreement signed on Jan. 15, 2021).
[90] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/banner/index.html) (resolution agreement signed on Jan. 06, 2021).
[91] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/elite-primary-care/index.html) (resolution agreement signed on Dec. 17, 2021).
[92] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ucmc/index.html) (resolution agreement signed on Nov. 12, 2020).

reasonable costs. Dr. Bhayani agreed to pay **$15,000** and comply with a Corrective Action Plan to address violations of HIPAA regulations regarding patient access to protected health information.[93]

- In October 2020, the HHS entered into a Resolution Agreement with Riverside Psychiatric Medical Group (RPMG) to settle charges that Riverside violated HIPAA when it failed to provide a patient with timely access to their medical records at reasonable costs. RPMG agreed to pay **$25,000** and comply with a Corrective Action Plan to address violations of HIPAA regulations regarding patient access to protected health information.[94]

- In October 2020, the HHS entered into a Resolution Agreement with The City of New Haven, Connecticut (New Haven) for violating HIPAA when it failed to terminate a former employee's access to PHI. New Haven's failure allowed the former employee to download PHI onto a USB drive and remove boxes containing documents from her old office. New Haven agreed to pay **$202,400** and comply with a Corrective Action Plan to settle the HIPAA violation charges.[95]

- In October 2020, the HHS entered into a Resolution Agreement with Aetna for violating HIPAA's Privacy and Security rules on three separate occasions. Aetna agreed to pay **$202,400** and comply with a Corrective Action Plan to settle the HIPAA violation charges.[96]

- In September 2020, the HHS entered into a Resolution Agreement with NY Spine to settle charges that NY Spine violated HIPAA when it failed to provide patients with timely access to their medical records at reasonable costs. NY Spine agreed to pay **$100,000** and comply with a Corrective Action Plan to settle the charges.[97]

- In September 2020, the HHS entered into a Resolution Agreement with a New Jersey-based hospital and medical center to settle charges that the Center violated HIPAA when it failed to provide a patient with timely access to their medical records at reasonable costs. Hospital agreed to pay **$160,000** and comply with a Corrective Action Plan to settle the charges.

[93] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/bhayani/index.html) (resolution agreement signed on Oct. 22, 2020).
[94] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/new-haven/index.html) (resolution agreement signed on Oct. 16, 2020).
[95] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/riverside/index.html) (resolution agreement signed on Oct. 13, 2020).
[96] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/aetna/index.html) (resolution agreement signed on Oct. 1, 2020).
[97] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/nyspine/index.html) (resolution agreement signed on Sep. 29, 2020).

- In September 2020, the HHS announced it settled the charges it brought against 5 companies for violating HIPAA when each company failed to provide individuals with timely access to their medical records as required under HIPAA's right of access provisions. HHS imposed a monetary penalty on the practices ranging from **$3,500 to $70,000**.[98]

- In June 2020, the HHS entered into a Resolution Agreement with The City of New Haven, Connecticut (New Haven) for violating HIPAA when it failed to terminate a former employee's access to PHI. New Haven's failure allowed the former employee to download PHI onto a USB drive and remove boxes containing documents from her old office. New Haven agreed to pay **$202,400** and comply with a Corrective Action Plan to settle the HIPAA violation charges.[99]

- In July 2020, the HHS entered into a Resolution Agreement with Athens Orthopedic Clinic (AOC) following an investigation into a breach incident where unauthorized parties gained access to AOC's IT system and were able to access the PHI of approximately 208,600 individuals. AOC agreed to pay **$1.5 million** and comply with a Corrective Action Plan to address violations of HIPAA regulations, including failures in risk analysis and security measures to protect PHI.[100]

- In March 2020, the HHS entered into a Resolution Agreement with Premera Blue Cross following an investigation into a breach incident where cyberattackers gained access to the ePHI of approximately 10.5 million individuals through Premera's information system. Premera agreed to pay **$6.85 million** and comply with a Corrective Action Plan to address violations of HIPAA regulations, including failures in risk analysis and security measures to protect ePHI.[101]

- In January 2017, Presence Health settled potential violations of the HIPAA Breach Notification Rule by paying **$475,000** and agreeing to implement a corrective action plan. Presence discovered that its paper-based operating room schedules, which contained the unsecured protected health information (PHI) of more than 800 individuals, were missing from an Illinois surgery center. Presence failed to notify, without unreasonable delay and within 60 days of discovering

[98] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/right-of-access-initiative/index.html) (press release dated Sep. 15, 2020).
[99] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/lifespan/index.html) (resolution agreement signed on Jun. 26, 2020).
[100] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/athens-orthopedic/index.html) (resolution agreement signed on Jul. 07, 2022).
[101] *See* HHS, (https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/premera/index.html) (resolution agreement signed on Mar. 30, 2022).

the breach, each of the affected individuals, prominent media outlets, and OCR, as required.[102]

- In October 2016, St. Joseph Health agreed to settle potential HIPAA violations, following a report that files containing electronic protected health information (ePHI) were publicly accessible through internet search engines from 2011 until 2012. The company agreed to pay a settlement of **$2.14 million** and adopt a comprehensive corrective action plan. The plan requires the organization to conduct an enterprise-wide risk analysis, develop and implement a risk management plan, revise its policies and procedures, and train its staff pursuant to the new plan.[103]

- In April 2016, a hospital agreed to settle potential violations of HIPAA, specifically the impermissible disclosure of two patients' protected health information (PHI) to news media and the lack of appropriate safeguards for PHI. The settlement included a payment of **$2.2 million** and the implementation of a comprehensive corrective action plan, including two years of monitoring.[104]

- In April 2016, a provider group practice agreed to settle charges that it had violated HIPAA by failing to execute a business associate agreement prior to turning over PHI of 17,300 individuals to a potential business partner, which included a payment of **$750,000** and the implementation of a corrective action plan.[105]

- In March 2016, a Minnesota health care system agreed to pay OCR **$1.55 million** and undertake certain corrective actions to settle potential violations of HIPAA's privacy and security requirements. Specifically, OCR was investigating whether the system had failed to execute a business associate agreement with a major contractor and whether it had failed to conduct an organizational risk analysis of the risks and vulnerabilities posed to electronic protected health information (ePHI).[106]

---

[102] *See* HHS Press Release, http://wayback.archive-it.org/3926/20170127111957/https://www.hhs.gov/about/news/2017/01/09/first-hipaa-enforcement-action-lack-timely-breach-notification-settles-475000.html.
[103] *See* HHS Press Release, https://wayback.archive-it.org/3926/20170127192714/https://www.hhs.gov/about/news/2016/10/18/214-million-hipaa-settlement-underscores-importance-managing-security-risk.html.
[104] http://www.hhs.gov/about/news/2016/04/21/unauthorized-filming-ny-med-results-22-million-settlement-new-york-presbyterian-hospital.html.
[105] http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/raleigh-orthopaedic-clinic/index.html.
[106] http://www.hhs.gov/about/news/2016/03/16/155-million-settlement-underscores-importance-executing-hipaa-business-associate-agreements.html.

- In March 2016, a research institution agreed to pay OCR **$3.9 million** to settle various potential violations of HIPAA and to undertake various corrective actions to address the potential non-compliance that triggered the investigation, which began after the ePHI of 13,000 individuals was stolen from an employee's car.[107]

- In February 2016, an administrative law judge ruled in favor of an OCR enforcement action, requiring a respiratory therapy provider to pay **$239,800** in civil money penalties (CMPs). OCR began its investigation of the provider after an employee left behind patient records after moving residences and discovered that the provider had inadequate policies and procedures to safeguard PHI taken offsite.[108]

- In December 2015, a university medical system agreed to pay **$750,000** to settle charges that it had failed to implement policies and procedures to prevent, detect, contain, and correct security violations. The investigation, initiated after a breach of roughly 90,000 individuals' PHI, indicated that the medical system's affiliated entities were not properly conducting risk assessments or responding to potential risks and vulnerabilities to the privacy and security of PHI. The system was also required to implement a corrective action plan and submit annual compliance reports to HHS.[109]

[107] http://www.hhs.gov/about/news/2016/03/17/improper-disclosure-research-participants-protected-health-information-results-in-hipaa-settlement.html.
[108] http://www.hhs.gov/about/news/2016/02/03/administrative-law-judge-rules-favor-ocr-enforcement-requiring-lincare-inc-pay-penalties.html.
[109] http://www.hhs.gov/about/news/2015/12/14/750000-hipaa-settlement-underscores-need-for-organization-wide-risk-analysis.html.

State Attorneys General Enforcement Actions

California

- In October 2025, the California Attorney General (CAG) reached a **$530,000** settlement with a streaming service provider Sling TV for alleged California Consumer Privacy Act (CCPA) violations related to opt-out failures and children's privacy.[110]

- On July 1, 2025, the California Attorney General announced a settlement with Healthline Media LLC, resolving allegations that its use of online tracking technology on Healthline.com violated the CCPA. An investigation that Healthline failed to allow consumers to opt out of targeted advertising and shared sensitive data with third parties without the necessary privacy protections. The settlement includes **$1.55 million** in civil penalties and mandates Healthline to implement strong injunctive terms, including a prohibition on sharing article titles that suggest a consumer may have a serious health condition. [111]

- In June 2024, the CAG announced Tilting Point Media LLC, a mobile video game developer, agreed to pay **$500,000** to settle the CAG's charges against it alleging it collected and shared children's data without first obtaining parental consent through a popular mobile app game in violation of the CCPA and the Children's Online Privacy Protection Act.[112]

- In a stipulated judgment announced in 2024, Blackbaud, Inc. agreed to pay **$6.75 million** to settle allegations of violating consumer protection and privacy laws stemming from a 2020 data breach. The breach involved the personal information of California residents stored by non-profit organizations using Blackbaud's products and services, including names, Social Security numbers, bank account information, and medical data. An investigation revealed that Blackbaud failed to implement reasonable data security measures, such as deleting outdated backup databases and utilizing multi-factor authentication, which allowed a threat actor to access and steal sensitive personal information. Furthermore, Blackbaud was found to have made misleading statements regarding the adequacy of its data security efforts before the breach and about the extent of the breach to its non-profit customers and the public. As part of

[110] *See* State pf California Department of Justice Office of the Attorney General Website, https://oag.ca.gov/news/press-releases/attorney-general-bonta-secures-530000-settlement-sling-tv-first-enforcement (press release dated Oct. 30, 2025).
[111] *See* CAG Website (https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-largest-ccpa-settlement-date-secures-155) (press release dated Jul. 1, 2025).
[112] *See* CAG Website, https://oag.ca.gov/news/press-releases/attorney-general-bonta-la-city-attorney-feldstein-soto-announce-500000 (press release dated Jun. 18, 2024).

the settlement, Blackbaud is also required to enhance its security protocols to better protect personal and protected health information.[113]

- In February 2024, DoorDash, Inc. agreed to pay **$375,000** to settle allegations that it sold customers' personal information without providing notice or the opportunity to opt-out, violating the CCPA and the California Online Privacy Protection Act. The investigation revealed that DoorDash participated in marketing co-operatives, which led to the unauthorized disclosure of customer data to non-participating businesses, including data brokers. As part of the settlement, DoorDash is also required to implement measures to prevent future violations, such as reviewing contracts with marketing vendors and utilizing technology to monitor the sale or sharing of consumer personal information.[114]

- On September 14, 2023, a global search engine provider agreed to pay **$93 million** to resolve allegations regarding its location-privacy practices, which were found to violate California consumer protection laws. A multi-year investigation determined that company misled users by collecting and using their location data for profiling and advertising without consent. The settlement also mandates that company enhance user transparency regarding location tracking, provide additional information when enabling location-related account settings, and undergo internal reviews for any significant changes affecting privacy disclosures.

- On August 24, 2022, Sephora, Inc. reached a stipulated judgment to pay **$1.2 million** to settle allegations of violating the California Consumer Privacy Act (CCPA). The Attorney General alleged that Sephora failed to inform consumers about the sale of their personal information and did not process opt-out requests via global privacy controls. The settlement also requires Sephora to enhance its online disclosures, provide opt-out mechanisms for consumers, and ensure compliance with CCPA in its service provider agreements.[115]

- In September 2020, Glow, Inc. and its parent company, Upward Labs Holdings, Inc., agreed to a **$250,000** settlement to resolve allegations that its fertility-tracking mobile app violated California's medical privacy and data security laws. An investigation found significant security flaws in the app, which stores sensitive data related to women's reproductive health. The settlement also mandates Glow to improve data security, consider the unique privacy impacts on

[113] *See* CAG Website, (https://oag.ca.gov/news/press-releases/attorney-general-bonta-secures-675-million-settlement-against-blackbaud-over) (press release dated Jun. 13, 2024).
[114] *See* CAG Website, (https://oag.ca.gov/news/press-releases/attorney-general-bonta-la-city-attorney-feldstein-soto-announce-500000).
[115] *See* CAG Website, (https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement).

women, obtain user consent before sharing sensitive information, and allow users to revoke consent.[116]

- On September 30, 2020, Anthem, a health insurance provider, agreed to pay **$8.69 million** to settle allegations related to a 2014 data breach that compromised sensitive personal information of over 78 million consumers, including 13.5 million Californians. The breach occurred due to phishing attacks that accessed Anthem's database containing names, Social Security numbers, and other personal details. The settlement also requires Anthem to enhance its data security measures to prevent future breaches.[117]

- In March 2016, a global financial institution paid **$8.5 million** to settle charges with the California Attorney General's Office that it had recorded consumers' phone calls without timely notification that they were being recorded. The bank also agreed to implement an internal compliance program to ensure that changes to its notification policy are made.

- In December 2015, the California Attorney General announced a **$25.95 million** settlement with a media and telecom company, who had allegedly unlawfully disposed of hazardous waste and discarded records without properly removing private consumer information. The company was also required to hire an independent auditor to conduct three environmental and privacy compliance audits over the five years following the settlement.

- In October 2015, Houzz, Inc., an online platform for home remodeling and design, paid **$175,000** to resolve allegations by the California Attorney General that the company violated California privacy laws. The company recorded incoming and outgoing telephone calls, intended for training and quality-assurance purposes, without notifying all parties on the call that they were being recorded. In addition to paying a monetary penalty, Houzz was required to appoint a Chief Privacy Officer and conduct a privacy risk assessment addressing its compliance efforts.[118]

- In September 2015, a global mass media, telecommunications, and entertainment conglomerate reached a **$33 million** settlement with the California Attorney General's Office over allegations that it posted online the names, phone numbers, and addresses of customers who had paid for unlisted voice over internet protocol (VOIP) phone service. In addition to providing

[116] *See* CAG Website, (https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-%E2%80%93).
[117] *See* CAG Website, (https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-869-million-settlement-against-anthem-inc).
[118] *See* CA AG Press Release, https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-settlement-houzz-inc-over-privacy.

refunds and restitution payments, the company is required to strengthen restrictions on its vendors' use of customer personal information and provide easy-to-read privacy disclosures to customers.

- In October 2014, the California Attorney General reached a **$28.4 million** settlement with a rental company over allegations that the company had violated California's consumer and privacy laws. The allegations included the charge that the company installed spyware on rented laptops allowing franchisees to remotely monitor keystrokes, capture screenshots, track the physical location of consumers, and activate the computer's webcam.[119]

- On May 8, 2025, the California Privacy Protection Agency (CPPA) ordered Jerico Pictures, Inc., a Florida-based data broker, to pay a **$46,000** fine for failing to register and pay an annual fee as mandated by California's Delete Act, which requires data brokers to delete user data upon user request. [120]

- On May 6, 2025, the CPPA ordered national clothing retailer Todd Snyder, Inc. to pay a **$345,178** fine and change its business practices to resolve allegations of violating the CCPA. The Enforcement Division found that Todd Snyder failed to properly oversee its privacy portal, resulting in a 40-day delay in processing consumer requests to opt out of the sale or sharing of personal information. Additionally, the company required consumers to submit excessive information and verify their identity before opting out. As part of the resolution, Todd Snyder must also enhance its privacy practices, including configuring its opt-out mechanisms and providing CCPA compliance training for employees. [121]

- On March 12, 2025, the CPPA ordered a Japanese car manufacturer to pay a **$632,500** fine and change its business practices to resolve claims of violating the CCPA. The investigation revealed that the company required Californians to verify their identity and provide excessive personal information to exercise privacy rights, that company used an inadequate online privacy management tool, and that company made it difficult for consumers to authorize others to act on their behalf. Additionally, the company shared personal information with ad tech companies without proper contracts to protect privacy. To address these issues, company must also implement a simpler process for asserting privacy rights, certify compliance, train employees, and consult a user experience designer to improve its privacy request methods.

---

[119] https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-reaches-284-million-settlement-rental-business.

[120] *See* California Privacy Protection Agency Website (https://cppa.ca.gov/announcements/2025/20250508.html) (press release dated May 8, 2025).

[121] *See* CPPA Website (https://cppa.ca.gov/announcements/2025/20250506.html) (press release dated May 6, 2025).

- On February 27, 2025, the CPPA reached a settlement with Background Alert, Inc., a California-based data broker, requiring the company to shut down operations until 2028 for failing to register and pay an annual fee as mandated by the Delete Act. The settlement follows an ongoing investigation into data broker compliance, and Background Alert faced allegations of creating and selling consumer profiles using billions of public records. The company was known for promoting its ability to uncover extensive personal information. Under the agreement, Background Alert **must cease operations for three years and could face a $50,000 fine** if it violates any terms of the settlement. [122]

- On February 20, 2025, the CPPA initiated an enforcement action against Jerico Pictures, Inc., a Florida-based data broker, seeking a **$46,000** fine for failing to register and pay an annual fee as required by the Delete Act. Jerico Pictures gained attention after a data breach exposed 2.9 billion records, including sensitive information like Social Security numbers. The Enforcement Division alleged that the company registered late and only after being contacted during the investigation.[123]

- On January 29, 2025, the CPPA's Enforcement Division announced a settlement with Key Marketing Advantage, LLC (KMA) for failing to register and pay an annual fee as required by the Delete Act. The CPPA's Board approved the settlement, which includes a **$55,800** fine for KMA, a Connecticut-based data broker, for not registering. KMA also agreed to pay the Enforcement Division's attorney fees for any future non-compliance. [124]

- On December 23, 2024, the CPPA's Enforcement Division announced settlements with two data brokers—PayDae, Inc. and The Data Group, LLC—for failing to register and pay an annual fee as required by the Delete Act. PayDae, a New York-based data broker, agreed to pay **$54,200**, while The Data Group, a Florida-based data broker, agreed to pay **$46,600**. Both companies also agreed to injunctive terms.[125]

- On November 14, 2024, the CPPA's Enforcement Division announced settlements with two data brokers, Growbots, Inc. and UpLead LLC, for failing to register and pay an annual fee as required by the Delete Act. Growbots agreed to pay **$35,400**, while UpLead agreed to pay **$34,400** to resolve the claims against

[122] *See* CPPA Website, (https://cppa.ca.gov/announcements/2025/20250227.html) (press release dated Feb. 27, 2025).
[123] *See* CPPA Website, (https://cppa.ca.gov/announcements/2025/20250220.html) (press release dated Feb. 20, 2025).
[124] *See* CPPA Website, (https://cppa.ca.gov/announcements/2025/20250129.html) (press release dated Jan. 29, 2025).
[125] *See* CPPA Website, (https://cppa.ca.gov/announcements/2024/20241223.html) (press release dated Dec. 23, 2024).

them. Both companies also agreed to injunctive terms, including covering the Enforcement Division's attorney fees for any future non-compliance. [126]

Colorado

- In September 2023, Colorado's Attorney General announced a **$60,000** settlement with Broomflield Skilled Nursing and Rehabilitation Center, LLC for failing to protect personal information belonging to patients and employees as part of a 2021 security breach. The settlement identified Broomfield lacked a data disposal policy, two factor authentication, and encryption of stored e-mails resulting in the loss of sensitive information, including SSNs, driver's license numbers, and bank account information.[127]

- In June 2021, Colorado's Attorney General announced a **$25,000** settlement with Impact Mobile Home Communities following a security breach affecting 15,000 residents. Bad actors used phishing tactics to access employee e-mail accounts containing sensitive personal information, including SSNs and financial details. Colorado's AG noted required Impact Home to implement comprehensive cybersecurity measures designed to prevent future incidents and enhance response times. The Colorado AG noted that it took Impact Home 10 months to notify affected individuals.[128]

Connecticut

- On August 13, 2024, the New York Attorney General, alongside the attorneys general of Connecticut and New Jersey, announced a **$4.5 million** settlement with Enzo Biochem, Inc. for failing to adequately protect the personal health information of approximately 2.4 million patients, including over 1.4 million New Yorkers. An investigation revealed that poor data security practices led to a ransomware attack, during which cybercriminals accessed Enzo's networks using shared employee login credentials. As part of the agreement, Enzo will pay $4.5 million, with New York receiving **$2.8 million**, and is required to implement enhanced cybersecurity measures, including multi-factor authentication, strong password policies, and regular risk assessments. Attorney General James emphasized the importance of data security in protecting patient safety.[129]

- In November 2015, the Connecticut Attorney General announced a **$90,000** settlement with a data storage company, which also required the company to

[126] *See* CPPA Website, (https://cppa.ca.gov/announcements/2024/20241114.html) (press release dated Nov. 14, 2024).
[127] https://coag.gov/app/uploads/2023/09/2023.08.31-Broomfield-Skilled-Nursing-Fully-Executed-AOD.pdf
[128] https://coag.gov/app/uploads/2021/06/AOD-Signed-Impact-MHC-and-Colorado-6.11.2021.pdf
[129] https://ag.ny.gov/press-release/2024/attorney-general-james-secures-45-million-biotech-company-failing-protect-new (press release dated Aug. 13, 2024).

implement additional training and information security measures. The attorney general's investigation began after a laptop containing the unencrypted PHI of nearly 9,000 Connecticut residents was stolen, resulting in a breach.[130]

Florida

- In October 2025, the Florida Attorney General filed an enforcement action against Roku, Inc. alleging several violations of Florida's Digital Bill of Rights in connection with monetization of children's data through data sharing partnerships and digital advertising.[131]

- In November 2023, the Florida Attorney General announced a **$6.5 million** settlement against Morgan Stanley for mishandling decommissioned devices. The complaint alleged Morgan Stanley potentially exposed millions of customer records through failure to properly dispose of devices containing unencrypted customer personal information (e.g., hard drives, servers), inadequate vendor controls, and allowing exposure of customer data.[132]

- In October 2014, the Florida Attorney General announced a **$850,000** multistate settlement with a bank over a data breach, resulting from the loss of unencrypted backup tapes and affecting approximately 260,000 customers. The settlement also required the bank to implement further compliance measures, ensuring that no backup tapes may be transported unless they are encrypted and security protocols are followed.[133]

Illinois

- In October 2020, Illinois's Attorney General announced a **$5 million** multi-state settlement with a health systems company after a 2014 data breach that impacted 6.1 million patients nationwide. The loss came after hackers accessed sensitive information about patients, including SSNs and birthdates. The settlement will require company to implement comprehensive information security policies designed to prevent future incidents and allow for faster response times.

Maryland

- In July 2022, the Maryland Attorney General announced an **$8 million** settlement with Wawa, Inc. for a 2019 data breach that compromised about 34

[130] http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=573262.
[131] https://www.myfloridalegal.com/sites/default/files/document_0002.pdf
[132] https://www.myfloridalegal.com/sites/default/files/2023-11/executed-morgan-stanley-avc-florida.pdf
[133] http://myfloridalegal.com/__852562220065EE67.nsf/0/DA5DA464904B7ED585257D730054E08B?Open&Highlight=0,breach.

million payment cards via malware extraction across its convenience store network and fueling stations.[134]

- In June 2014, the Maryland Attorney General announced a **$100,000** settlement with an app development company for alleged deceptive trade practices and COPPA violations. The company allegedly misled consumers regarding the level of privacy that they could expect and by not disclosing to consumers the fact that the app collected and maintained names and phone numbers from electronic contact lists. Finally, the attorney general alleged that the company had violated COPPA by knowingly collecting personal information from children without adequate consent. Along with the financial penalty, the app company agreed to take corrective compliance actions to address the allegations.[135]

Massachusetts

- In August 2025, the Massachusetts Attorney General reached a settlement with Peabody Properties, Inc., for **$795,000** for failing to adequately protect the personal information of several thousand residents and unlawfully delaying notice to affected consumers. Peabody experienced five separate cybersecurity breaches based on phishing intrusions exposing SSNs, driver's license numbers, and bank account details.[136]

- In January 2015, the Massachusetts Attorney General, joined by other state attorneys general, announced a **$106,000** settlement with an online retailer following a breach of residents' personal information. Along with the cash settlement, the retailer was required to implement security measures to protect consumer information and provide the attorneys general compliance reports for two years.[137]

- In December 2014, the Massachusetts Attorney General announced a **$825,000** settlement with a large bank, also requiring the bank to implement more stringent security measures. The investigation was initiated after the bank lost the personal information of more than 90,000 state residents contained on back-up tapes and delayed its notice of the breach to the Massachusetts Attorney General.[138]

New York

[134] https://www.naag.org/wp-content/uploads/2025/11/2022.07.26-NJ-Press-Release.pdf
[135] https://www.oag.state.md.us/Press/2014/061214.html. 0
[136] https://www.mass.gov/news/ag-campbell-reaches-795000-settlement-with-property-management-company-for-failing-to-protect-the-personal-information-of-thousands-of-massachusetts-residents
[137] http://www.mass.gov/ago/news-and-updates/press-releases/2015/2015-01-07-zappos-settlement.html.
[138] http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-12-08-td-bank.html.

- On March 7, 2025, the New York Attorney General (NYAG) announced a **$650,000** settlement with Saturn Technologies, developer of the Saturn app, which is used by high school students, for failing to protect high school users' privacy. An investigation revealed that Saturn did not adequately verify users' school email addresses or ages, allowing interactions between high school students and unverified individuals outside of their high school communities. The company also made user verification optional without notifying users and used inadequate methods for confirming high school affiliation. As part of the settlement, Saturn Technologies must enhance privacy measures, notify users about verification changes, and limit the visibility of non-Saturn users' information.[139]

- On January 28, 2025, the NYAG announced a settlement securing **$450,000** from three companies which sell home security video cameras and related home security products, including Fantasia Trading LLC and Smart Innovation, LLC — for failing to adequately secure consumers' private home security video footage. An investigation revealed that video streams were not always securely encrypted, allowing unauthorized access to footage via shared links. The settlement mandates that the companies implement stronger data protection measures and pay the penalty. [140]

- On December 19, 2024, the NYAG announced a settlement with Noblr, a United States-based auto insurance company, for allegedly maintaining poor data security which allowed scammers to steal the personal information, such as driver's license numbers and dates of birth, of over 80,000 New Yorkers. The scammers used this stolen personal information to file fraudulent unemployment claims. As part of the settlement, Noblr was required to enhance web application defenses, maintain comprehensive information security program designed to protect the security, confidentiality, and integrity of private information, develop and maintain a data inventory of private information, maintain reasonable authentication procedures for access to private information, and maintain a logging and monitoring system to alert on suspicious activity.[141]

- On December 9, 2024, the NYAG announced a settlement with HealthAlliance, a health care facility operator, for allegedly failing to protect personal and medical data of over 240,000 consumers. HealthAlliance's failure to protect this data led

[139] https://ag.ny.gov/press-release/2025/attorney-general-james-announces-settlement-app-developer-failing-protect-young.
[140] https://ag.ny.gov/sites/default/files/settlements-agreements/state-of-new-york-v-fantasia-training-llc-aod-2025.pdf.
[141] (https://ag.ny.gov/press-release/2024/attorney-general-james-secures-500000-auto-insurance-company-over-data-breach) (press release dated Dec. 19, 2024).

to a cyberattack, during which cyber-attackers were able to steal information such as names, addresses, dates of birth, Social Security numbers, diagnoses, lab results, medications, health insurance information, provider names, dates of treatment, and/or financial information. HealthAlliance agreed to pay **$550,000** to settle the charges and agreed to adopt procedures designed to strengthen its cybersecurity practices.[142]

- On November 25, 2024, the NYAG announced that it settled its charges against Geico and Travelers' Insurance, two United States-based auto insurance companies, **for $11.3 million** for the companies' failures to maintain adequate data security. The companies' failures allowed data security hackers to steal personal data such as driver's license numbers, which the hackers used to file fraudulent unemployment claims. As part of the settlement, both companies also agreed to enhance their data security practices. [143]

- On November 15, 2024, the NYAG announced that National Amusements Inc., a United States-based movie theater operator, agreed to pay **$250,000** to settle the NYAG's charges against it for allegedly failing to protect its employees' personal information. National Amusement's alleged failure allowed a hacker to steal the employee credentials and personal information, such as names, dates of birth, Social Security numbers, passport numbers, financial account numbers, driver's license numbers, and health insurance account numbers, of over 82,000 employees. National Amusement also allegedly failed to inform affected employees of the breach for over a year. As part of its settlement, National Amusement also agreed to adopt various cybersecurity measures to strengthen its network's cybersecurity.[144]

- On October 29, 2024, the NYAG announced a **$2.25 million** settlement with Albany ENT & Allergy Services, P.C. (AENT) for failing to protect the personal information of over 200,000 patients during two ransomware attacks in 2023. AENT did not maintain adequate cybersecurity measures and delayed its response to the breaches. The settlement requires AENT to pay **$500,000** in penalties and invest $2.25 million over five years to improve its information security practices. Additionally, AENT will provide affected individuals with one

[142] https://ag.ny.gov/press-release/2024/attorney-general-james-secures-550000-hudson-valley-health-care-facility (press release dated Dec. 9, 2024).
[143] https://ag.ny.gov/press-release/2024/attorney-general-james-and-dfs-superintendent-harris-secure-113-million-auto (press release dated Nov. 25, 2024).
[144] https://ag.ny.gov/press-release/2024/attorney-general-james-secures-250000-movie-theater-operator-failing-protect (press release dated Nov. 15, 2024).

year of free credit monitoring and implement a comprehensive cybersecurity program.[145]

- On February 13, 2024, the NYAG announced a **$750,000** settlement with College Board for violating students' privacy by unlawfully licensing personal data collected during PSAT, SAT, and AP exams. The investigation revealed that College Board had improperly licensed the information of over 237,000 New York students in 2019 and used their data for marketing purposes. As part of the settlement, College Board will pay $750,000 in penalties and is prohibited from monetizing student data obtained through contracts with New York schools. Attorney General James emphasized the need for organizations to protect students' personal information rather than exploit it for profit.[146]

- On December 27, 2023, the NYAG announced a **$300,000** settlement with The New York-Presbyterian Hospital (NYP) for improperly disclosing health information of website visitors. An investigation revealed that NYP used advertising tools that collected and shared personal information with third-party tech companies, violating the Health Insurance Portability and Accountability Act (HIPAA). As part of the settlement, NYP will implement new policies to secure the deletion of protected health information and enhance privacy safeguards. The NYAG emphasized the need for hospitals to protect patients' personal data, stating that patients should be able to seek medical help without compromising their privacy.[147]

- On November 16, 2023, the NYAG and a coalition of five attorneys general announced a **$6.5 million** settlement with Morgan Stanley Smith Barney LLC for compromising the personal information of millions of customers. The investigation revealed that Morgan Stanley failed to properly decommission computers and erase unencrypted data before auctioning them, which included information belonging to 1.1 million New Yorkers. As part of the agreement, New York will receive $1,658,047, and Morgan Stanley is required to strengthen its data security measures. The NYAG emphasized the importance of companies taking responsibility for protecting customer data, stating that personal information should not be sold off due to negligence. Morgan Stanley will also implement provisions to enhance its cybersecurity.[148]

[145] https://ag.ny.gov/press-release/2024/attorney-general-james-secures-225-million-capital-region-health-care-provider (press release dated Oct. 29, 2024).
[146] https://ag.ny.gov/press-release/2024/attorney-general-james-and-nysed-commissioner-rosa-secure-750000-college-board (press release dated Feb. 13, 2024).
[147] https://ag.ny.gov/press-release/2023/attorney-general-james-secures-300000-newyork-presbyterian-hospital-failing (press release dated Dec. 27, 2023).
[148] https://ag.ny.gov/press-release/2023/attorney-general-james-and-multistate-coalition-secure-65-million-morgan-stanley (press release dated Nov. 16, 2023).

- On November 8, 2023, the NYAG secured a **$450,000** settlement from US Radiology Specialists, Inc. for failing to protect patients' personal and health care data. An investigation found that US Radiology did not prioritize upgrading its hardware, leaving its network vulnerable to a ransomware attack that affected over 92,000 New Yorkers. As part of the agreement, US Radiology will pay the penalties and is required to update its IT infrastructure and enhance its data security policies. The NYAG emphasized the importance of safeguarding patient information, urging companies to make necessary upgrades to protect against cyber threats. US Radiology will implement additional security measures, including encrypting personal information and maintaining a penetration testing program to identify vulnerabilities.[149]

- On October 18, 2023, the NYAG secured a **$350,000** settlement from Personal Touch Holding Corporation for failing to protect the personal and health care data of approximately 316,845 New Yorkers. The investigation revealed that Personal Touch's inadequate data security measures made it vulnerable to a ransomware attack, violating state law and HIPAA regulations. As part of the agreement, Personal Touch will pay the penalties, enhance its cybersecurity infrastructure, and provide free credit monitoring and identity theft services to affected individuals. The NYAG emphasized the responsibility of healthcare institutions to safeguard patient information. In a separate agreement, an insurance software vendor, Falcon Technologies, will pay $100,000 for compromising Personal Touch employees' data. Personal Touch also agreed to implement various security measures, including regular risk assessments, encryption of personal information, and enhanced employee training.[150]

- On October 5, 2023, the NYAG and a coalition of 50 attorneys general announced a **$49.5 million** settlement with *Blackbaud*, a cloud company, over a significant data breach that affected thousands of nonprofit institutions, including charities and educational organizations. The breach, which occurred in 2020, exposed the personal information of millions of donors and constituents, including sensitive data such as Social Security numbers and financial information. As part of the settlement, Blackbaud will pay $49.5 million, with New York receiving **$2.9 million,** and will overhaul its data security and breach notification practices. The NYAG emphasized the importance of protecting personal information and holding companies accountable for inadequate security measures. Blackbaud is required to implement enhanced security

[149] https://ag.ny.gov/press-release/2023/attorney-general-james-secures-450000-medical-company-providing-services-western (press release dated Nov. 8, 2023).
[150] https://ag.ny.gov/press-release/2023/attorney-general-james-secures-350000-long-island-home-health-care-company (press release dated Oct. 18, 2023).

protocols, including total database encryption, improved incident response plans, and third-party compliance assessments for seven years.[151]

- On May 25, 2023, the NYAG secured a **$300,000** settlement from *Sports Warehouse Inc*., an online sporting goods retailer, for failing to protect the personal data of 2.5 million consumers. The breach, which occurred in 2021, compromised sensitive information, including credit card details and email addresses for over 136,000 New Yorkers. As part of the agreement, Sports Warehouse will pay $300,000 in penalties and enhance its cybersecurity measures. The NYAG emphasized the importance of safeguarding consumer information, stating that online shoppers should not have to worry about their data being compromised. Sports Warehouse is required to implement a comprehensive information security program, encrypt consumer data, strengthen password requirements, and improve data retention practices.[152]

- On October 12, 2022, the NYAG secured **a $1.9 million** settlement from *Zoetop Business Company, Ltd.* for mishandling a data breach that compromised the personal information of 39 million SHEIN and 7 million ROMWE customers, including over 800,000 New Yorkers. The investigation revealed that Zoetop failed to safeguard consumer data and downplayed the breach's scope, misleading customers about the extent of the incident. The breach exposed sensitive information, including credit card details and personal identifiers. As part of the settlement, Zoetop will pay the penalties and is required to strengthen its cybersecurity measures. The NYAG emphasized that companies must take data protection seriously and be transparent with consumers regarding breaches.[153]

- On June 23, 2022, the NYAG, along with 45 other attorneys general, announced a **$1.25 million** settlement with *Carnival Cruise Line* for compromising the personal information of 180,000 employees and customers due to inadequate security practices. The breach, which occurred in 2019, affected 6,575 New Yorkers and involved sensitive data, including names, addresses, and payment information. As part of the settlement, Carnival will pay New York **$44,092.12** in penalties and is required to enhance its email security and breach response measures. The NYAG emphasized the need for companies to strengthen data privacy practices to protect consumers from fraud. Carnival's commitments include implementing

[151] https://ag.ny.gov/press-release/2023/attorney-general-james-and-multistate-coalition-secure-495-million-cloud-company (press release dated Oct. 5, 2023).
[152] https://ag.ny.gov/press-release/2023/attorney-general-james-secures-300000-online-sporting-goods-retailers-failing (press release dated May 25, 2023).
[153] https://ag.ny.gov/press-release/2022/attorney-general-james-secures-19-million-e-commerce-shein-and-romwe-owner-zoetop (press release dated Oct. 12, 2022).

multi-factor authentication, conducting employee training, and undergoing independent security assessments.[154]

- In May 2017, the New York Attorney General announced a settlement with a wireless security company that failed to secure users' passwords and other credentials. A group of independent security researchers found that *Safetech*, which sells Bluetooth-enabled doors and padlocks, transferred passwords to consumers' phones and other devices without encryption, leaving users susceptible to hacking and theft. After the attorney general's investigation, Safetech agreed to encrypt all passwords and other credentials in its locks, prompting users to change the default password upon initial setup and establish a comprehensive security program.[155]

- In March 2016, the New York Attorney General announced a **$95,000** settlement with a uniform supply company and its web developer for the disclosure of more than 500 social security numbers over the internet. The investigation began after the attorney general received a tip that job applicants' personal information, including their Social Security numbers, could be found via a simple internet search. The attorney general also noted that the company took nearly a month to notify affected individuals and the attorney general's office. In addition to the cash penalties, the company and developer agreed to implement additional information security measures.[156]

- In January 2016, the New York Attorney General announced a settlement with an online transportation network over charges that it had inadequately protected consumer information and had failed to make timely notification to the attorney general and individuals following a data breach. The company agreed to implement several security-enhancing measures and paid a penalty of **$20,000**.[157]

Texas

- In October 2025, the Texas Attorney General finalized a **$1.375 billion** settlement with a global search engine provider over privacy claims from two 2022 lawsuits. The lawsuits centered around company's handling of geolocation

[154] https://ag.ny.gov/press-release/2022/attorney-general-james-recovers-125-million-consumers-affected-carnival-cruise (press release dated Jun. 23, 2022).
[155] *See* NY AG Press Release, https://ag.ny.gov/press-release/ag-schneiderman-announces-settlement-tech-company-over-sale-insecure-bluetooth-door.
[156] http://www.ag.ny.gov/press-release/ag-schneiderman-announces-settlement-after-social-security-numbers-over-500-job.
[157] http://www.ag.ny.gov/press-release/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy.

data, incognito browsing activities, and biometric identifiers including voiceprints and facial records.

- On July 30, 2024, the TAG announced it settled charges with a global social media platform for capturing, without authorization, the biometric data of its users — which included millions of Texans. The TAG accused company of unlawfully collecting biometric data without informed consent, violating both the CUBI and the Deceptive Trade Practices Act. Since 2011, company had used facial recognition software on photos uploaded by Texans, capturing facial geometry records without their knowledge. The settlement requires the company to pay Texas **$1.4 billion** over five years.

Utah

- In January 2022, the Utah Attorney General reached a settlement with a senior living and healthcare management company for **$200,000** following a 2019 data breach impacting both patients and employees in Utah and Oregon. The data breach occurred after an Avalon employee fell victim to a phishing scam, and scammers accessed names, SSNs, dates of birth, driver's license numbers, medical treatment information, and certain financial information.[158]

Washington

- In January 2025, the Washington Attorney General filed enforcement action against T-Mobile for failing to adequately protect sensitive personal information of more than 2 million residents. This after bad actors gained access to company internal network and exposed personal information belonging to 79 million consumers nationwide.[159] "This significant data breach was entirely avoidable," and "T-Mobile had years to fix key vulnerabilities in its cybersecurity systems – and it failed," according to the press release.

[158] https://www.naag.org/wp-content/uploads/2025/07/2022.12.27-OR-Press-Release.pdf
[159] https://agportal-s3bucket.s3.us-west-2.amazonaws.com/uploadedfiles/Home/News/Press_Releases/FINAL%20T-Mobile_Complaint.pdf?VersionId=1S7AbxiAfKV_mlkDU8mkGpN8sEQQxsIU