WASHINGTON STATE ATTORNEY GENERAL'S OFFICE

2024

DATA BREACH REPORT

LETTER FROM THE ATTORNEY GENERAL

November 2024

Dear Washingtonians,

This is the ninth annual Data Breach Report published by my office. This year's report reveals that the number of data breach notifications annually sent to Washingtonians is rapidly increasing. For the first time ever, the number of notifications sent to Washingtonians in a single year exceeded the state's population.[1] With nearly a decade of trend data available, it is undeniable that significant changes to policies and industry practices are needed to curtail the growing frequency and intensity of data breaches affecting Washingtonians.

In the last year, our office received 279 data breach notices, resulting in just over 11.6 million data breach notices sent to Washingtonians. This is five million more than the previous all-time high of 6.5 million notices in 2021.

These statistics further underscore our state's critical need for comprehensive data privacy regulation. We live in an internet-driven economy that relies on the mass collection and retention of our personal information. Data breaches are symptomatic of gaps in data privacy policies and the standards and practices of every entity that collects or controls this information. As such, this report includes recommendations addressing both data breaches and data privacy. These include shortening the notification deadline, adding to the definition of personal information, and improving transparency in the data economy.

We will continue to enforce the law, and to provide Washingtonians information to protect your business and your data from the intensifying threat of data breaches.

Sincerely,

Bob Ferguson
Washington State Attorney General

Executive Summary

- 2024 represents the single highest total number of data breach notices sent to Washingtonians (11.6 million) since 2016.
    - This is up significantly from 2023 (4.5 million). The previous record was 6.5 million in 2021.

- The Attorney General's Office (AGO) received 279 data breach notifications in 2024 - the second highest recorded amount since 2016.
    - This is also up from 2023 (178). The record is 286 notices in 2021.

- Cyberattacks, particularly ransomware attacks, were again the most common type of breaches.
    - Cyberattacks caused 78% of all reported breaches, compared to 67% in 2022 and 64% in 2023.
    - 113 breaches were caused by ransomware attacks. This is up from 2023 (66).
    - Ransomware attacks accounted for 52% of all cyberattacks (113 of 217) and more than a third of all breaches (41%).

Background

A data breach is the unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by a person, business, or agency. Washington law requires entities impacted by a data breach to notify Washingtonians whose personal information is compromised, as well as to notify the AGO if the breach impacts more than 500 Washingtonians.

In 2019, Attorney General Ferguson proposed, and the Legislature passed, a bill strengthening Washington's data breach notification law. This legislation significantly expanded the definition of personal information, required notices to consumers to include the period of time their data was at risk, and reduced the deadline to provide notice to consumers to 30 days after the discovery of a breach. These changes went into effect on March 1, 2020.

This report is based on data breach notifications received by the AGO between July 24, 2023 and July 23, 2024 that affected more than 500 Washingtonians' personal information. Additional information on our data gathering and analysis process can be found in the appendix on page 16, or online at: https://www.atg.wa.gov/data-breach-live-statistics.

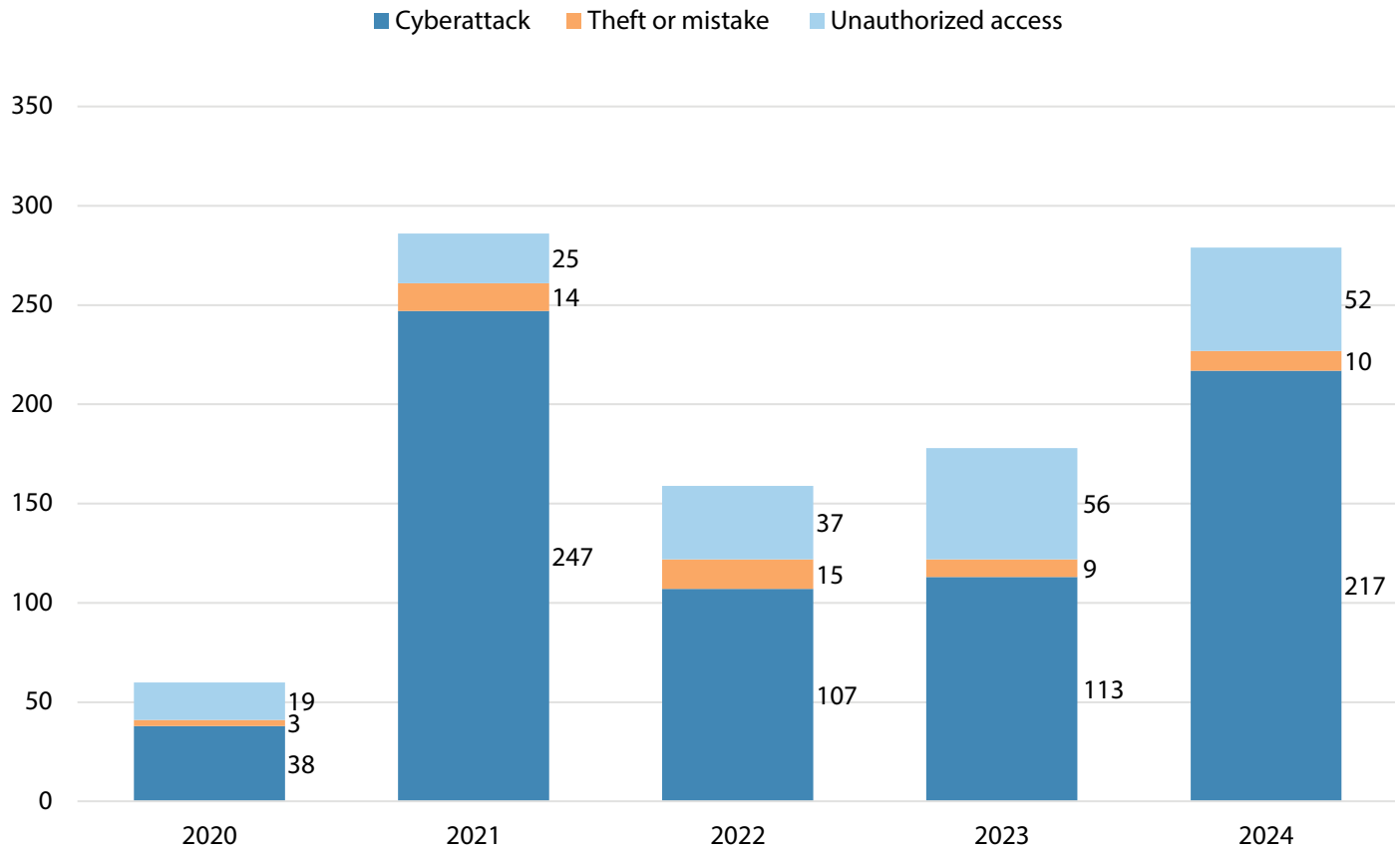
Recommendations

In order to provide consumers with more transparency and control over how and where their data is collected, stored, and shared, the AGO recommends that policymakers:

1. Make improvements to the state's data breach notification law by:
    a. Reducing the data breach notification deadline to three days;
    b. Creating language access requirements for data breach notifications; and
    c. Expanding the definition of "personal information" in RCW 19.255.005 to include (a) Individual Tax Identification Numbers (ITINs) and (b) full name in combination with a redacted Social Security Number (SSN) that still exposes the last four digits of the number.
2. Require businesses to recognize and honor opt-out preference signals and give Washingtonians more control over how their data is collected and used;
3. Require transparency from data brokers and data collectors; and
4. Consult with Tribes on how best to support their efforts in combatting cyberattacks.

For detailed information on each of these recommendations, please see the "Recommendations" section beginning on page 9.

Total Number of Data Breaches by Cause

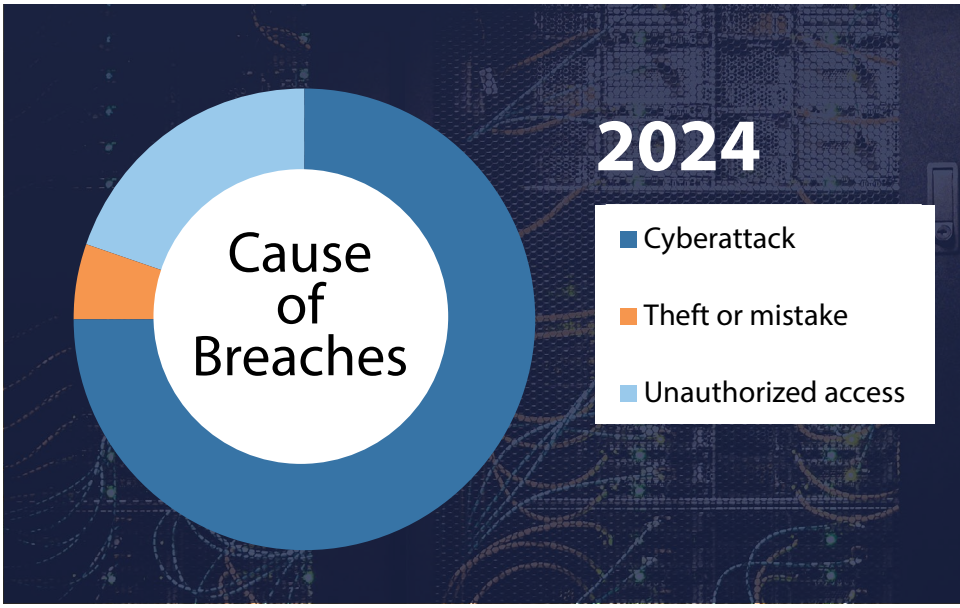


Data breaches fall into three broad categories:

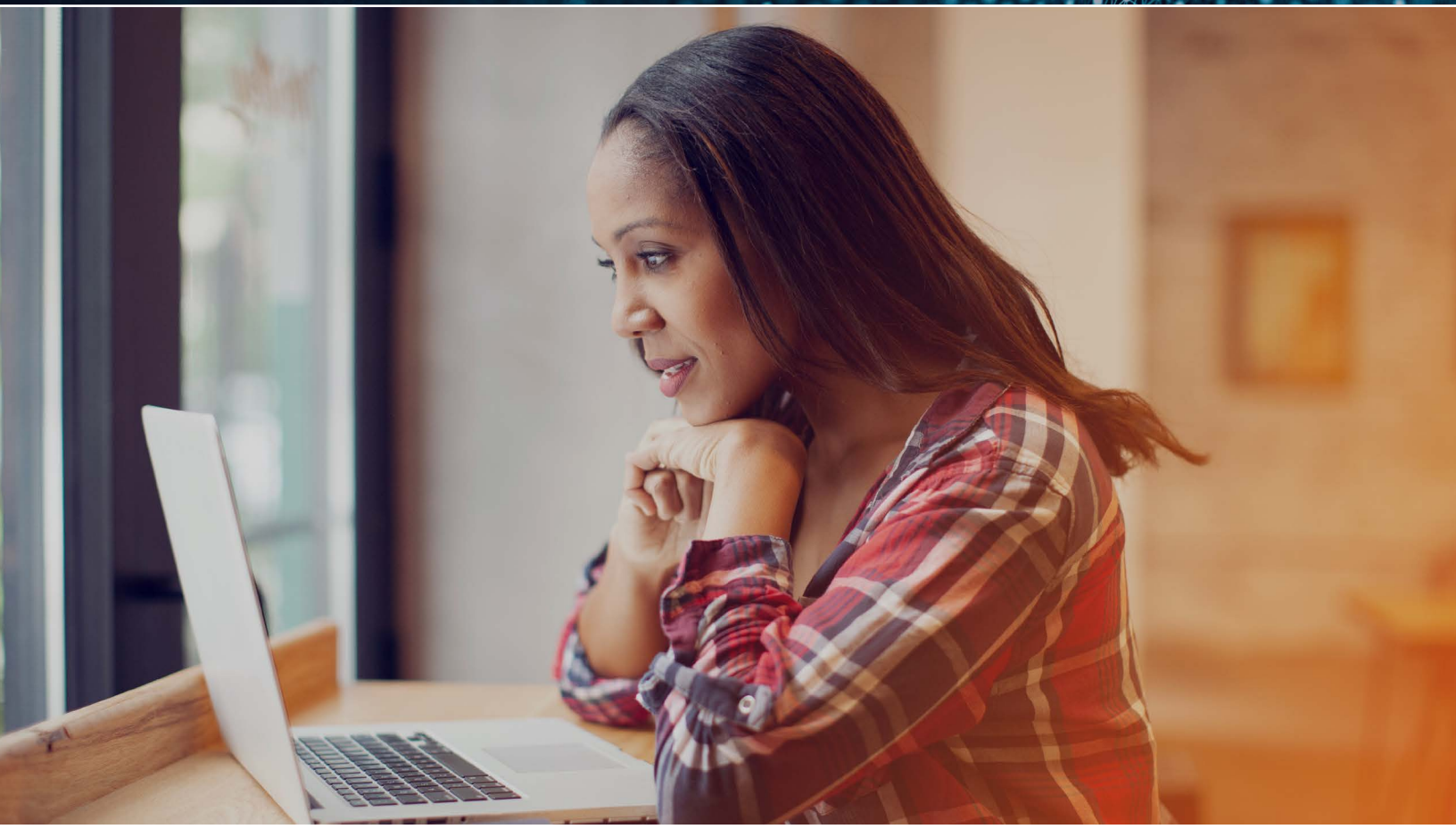
1. **Cyberattack**: A third party deliberately attempts to access secured data, such as information stored on a server, using cyber technology. The attack can use a skimmer, spyware, phishing email, ransomware, or similar means of accessing secure data remotely.

2. **Theft or mistake**: The mistaken loss of information, such as a clerical error that sent W-2 information to an unintended recipient, or the inadvertent theft of information, such as stealing a laptop that happened to contain patient medical records.

3. **Unauthorized access**: An unauthorized person purposefully accesses secure data through means such as an unsecured network or sifting through sensitive documents left out on a desk.



A Closer Look at Cyberattacks



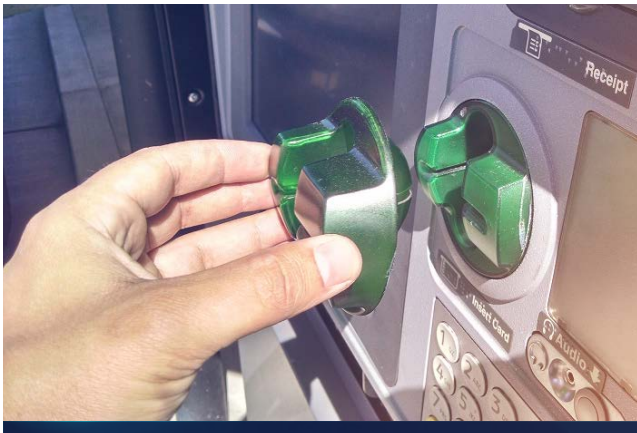
Cyberattacks can occur in a number of ways. Some of the most common methods include:

- **Malware**: The installation of malicious code onto a website, server, or network in order to disrupt the system or covertly obtain access to the data held within.

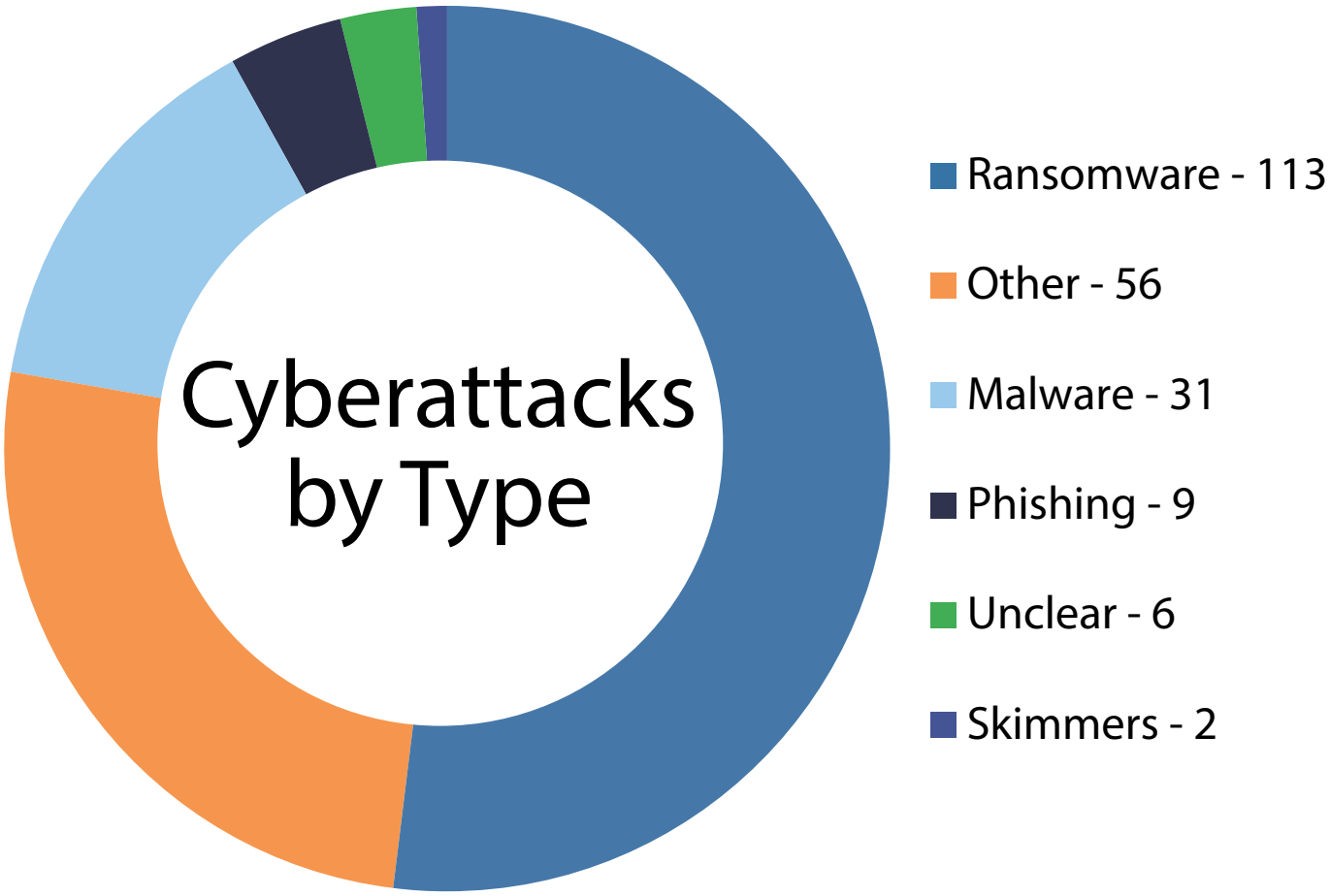
- **Ransomware**: A unique type of malware that holds data hostage while seeking a ransom payment from the breached entity. Typically, cybercriminals insert malicious code that encrypts data into an entity's network, thus locking the entity out of their own data.

- **Phishing**: The practice of sending a fraudulent communication, often via email, that appears to be from a financial institution, government, employer, or other entity in order to fool the recipient into providing their information or to download malware through an attachment or included link.

- **Skimmers**: A malicious card reader attached to payment terminals, such as those at an ATM or gas station, which collects data on cards inserted into the terminal. Often, cybercriminals will use the skimmer in conjunction with a device to record PIN information, such as a fake PIN pad or hidden camera.



A skimmer being installed on an ATM
Source: Washington State Department of Financial Institutions

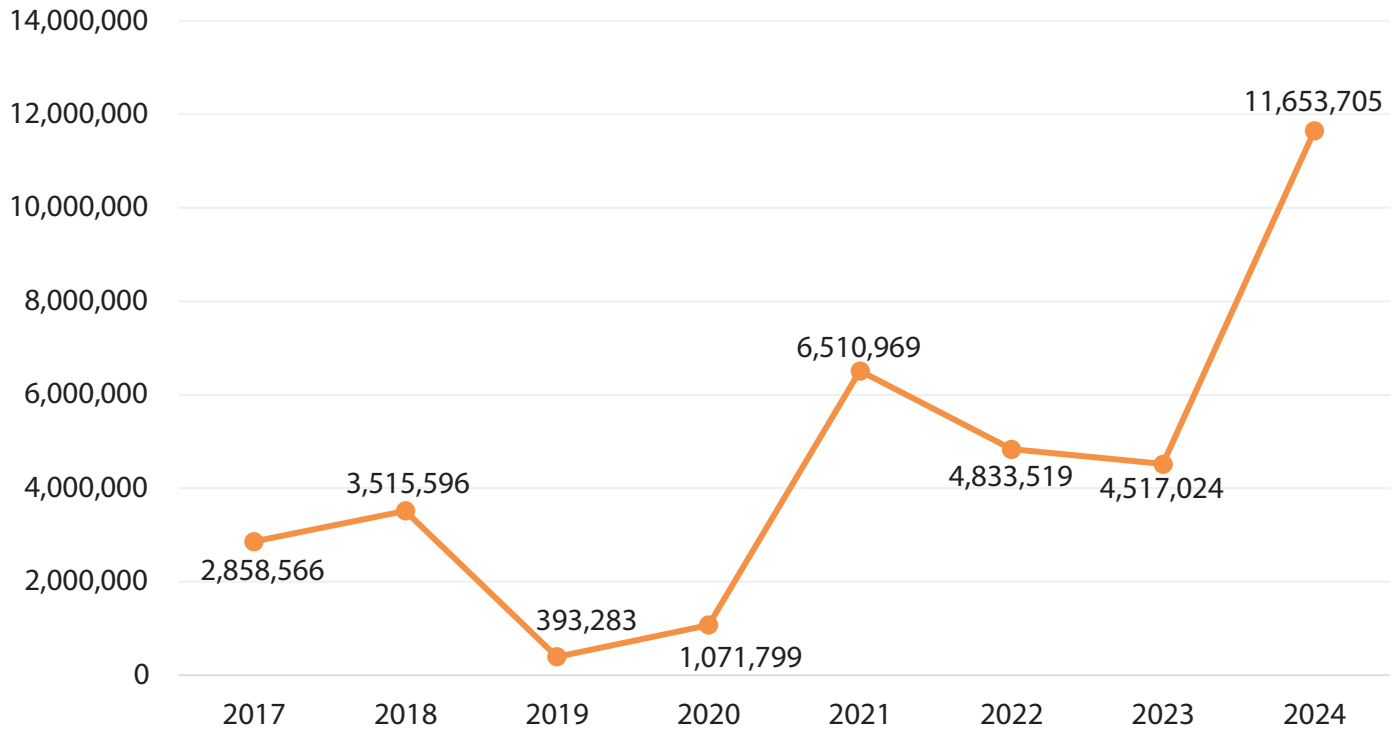


Our office was notified of 217 breaches caused by cyberattacks in 2024. Of those 217 breaches, six notices did not provide enough information to discern the specific method of cyberattack used. The most common cyberattack type was ransomware, which represented 52% (113 of 217) of cyberattacks.

This is the fourth consecutive year in which ransomware attacks were the most common type of cyberattack. Since 2021, ransomware attacks have resulted in an average of 2.1 million data breach notices per year. This ranks first among all types of cyberattacks over this time. Additionally, private businesses have experienced the most ransomware attacks during this period (31 per year), followed by: Non-profit/charity (18 per year), Healthcare (17 per year), Education (14 per year), Finance (12 per year), and Government (two per year).

Overall, businesses reported 112 breaches to our office in 2024. Among all businesses, telecommunications sent the most data breach notices to consumers (3.4 million) - the vast majority of these came from the mega breach of Comcast (3.1 million). This was followed by hospitality (821 thousand) and entertainment (804 thousand). Excluding the "other" category, retail reported the most data breach incidents (20 breaches) but represented only a small fraction of the notices sent to consumers in 2024 (88 thousand).

Annual Number of Washingtonians Affected by Data Breaches



In 2024, 279 data breaches that affected more than 500 Washingtonians' personal information were reported to the AGO. This is up from 178 breaches in 2023. The total number of Washingtonians affected increased as well – up 158% from last year, from 4,517,024 to 11,653,705. Some statistics that stand out include:

- The overall number of reported breaches has increased significantly and represents the second highest total recorded in Washington at 279 breaches;
- The number of breaches impacting more than 50,000 Washingtonians is in double digits for the fourth straight year, and for the first time exceeded more than 20 such breaches in a single year (25); and
- The overall number of Washingtonians affected increased massively from 2023, including two mega breaches affecting more than one million Washingtonians (Comcast and Fred Hutchinson Cancer Center). This is the first time more than one mega breach was reported in a single year.

The 11,653,705 data breach notices sent in 2024 represent the highest total sent to Washingtonians in a single year since our office began tracking this information. This is also the first time that the total number of notices sent exceeded the total population of the state (approximately eight million residents), suggesting that millions of Washingtonians experienced multiple breaches of their personal information within a single calendar year (see "Data Analysis Methodology and Limitations" on page 16 for more information on how this is possible). This year's numbers leave little doubt that data breaches continue to be an active and significant threat to consumers' privacy, security, and finances.

Types of Personal Information Compromised

Washington law requires notification to the AGO when a data breach includes personal information (PI). Washington defines PI as:[2]

An individual's first name or first initial and last name in combination with any of the following:

Social Security number;

Driver's license number or Washington identification card number;

Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to their account, or any other numbers or information that can be used to access a person's financial account;

Student, military, or passport identification numbers;

Health insurance policy or identification numbers;

Full date of birth;

Private keys for electronic signature;

Medical information, including medical history, mental or physical condition, diagnoses, or treatment; or

Biometric data.

OR

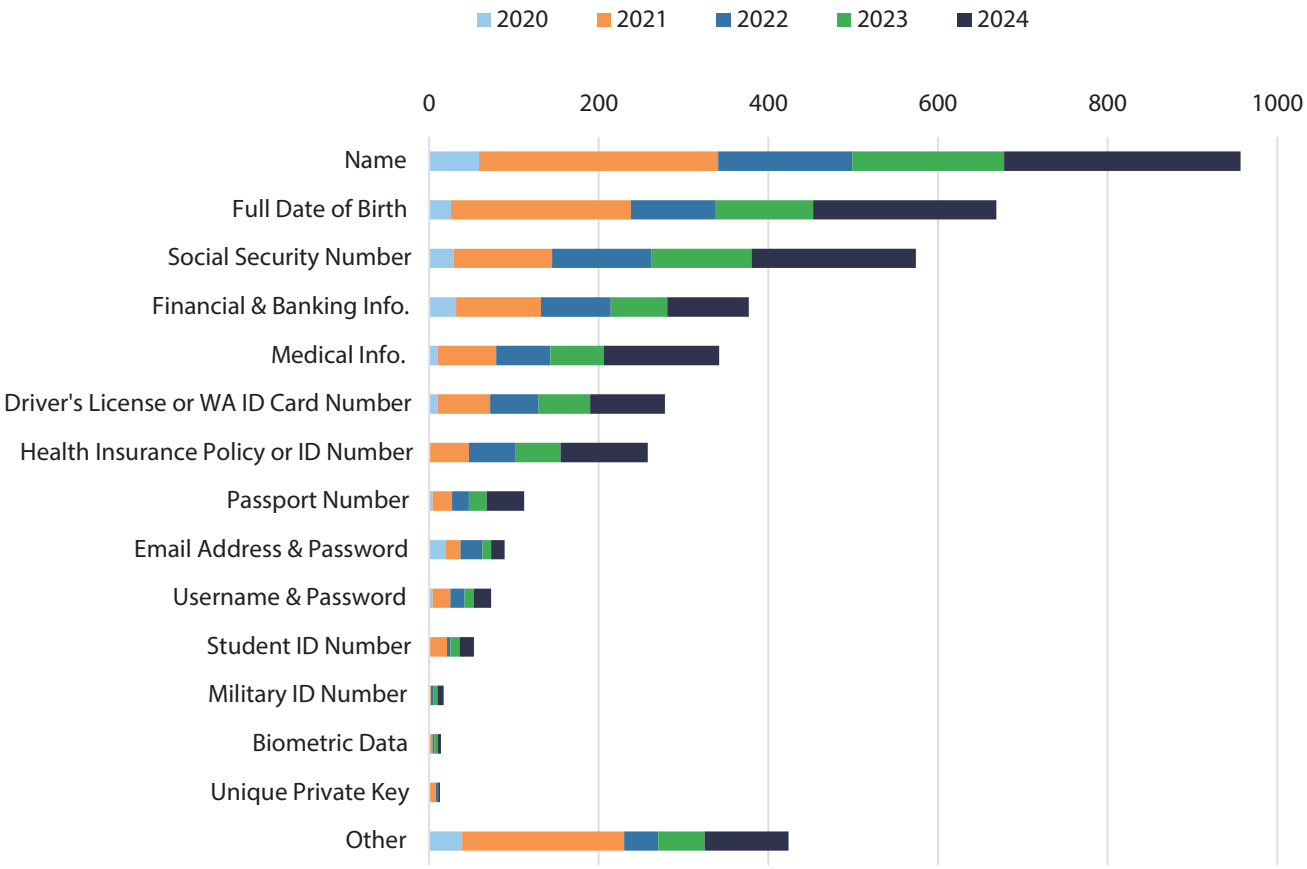
An individual's username or email address in combination with a password or security questions and answers that would permit access to an online account.

Additionally, any of the above elements, not in combination with first name or initial and last name, are considered PI if the affected data was not encrypted or redacted and would enable a person to commit identity theft against the consumer.

In 2024, 194 breaches, representing just over two-thirds (69.5%) of all breaches reported, resulted in the compromise of a Washingtonian's Social Security number (SSN). SSNs have been among the top three most compromised pieces of PI in every report since 2016. This is likely due to the value of SSNs to hackers and would-be identity thieves, as they are often required for individuals to access financial products, such as loan applications or government services and benefits, like Medicare.

Overall, full date of birth (216) leads as the most commonly compromised piece of PI for the second time in the last four years. This again makes sense, as date of birth is often required to validate an individual's identity for a number of services and products. While a full date of birth may not seem like the most sensitive piece of information, in combination with any of the other categories above - such as SSNs - the acquisition of a full date of birth could be of great consequence, and a huge boon to identity thieves.

Personal Information Exposed by Data Breaches



1. Make Improvements to the State's Data Breach Notification Laws

Our state's data breach notification laws were last updated in 2019 and went into effect on March 1, 2020. In the five years since those amendments, the data economy and the threats posed to Washingtonians' data have evolved significantly, from the rapid rise in ransomware attacks to advances in generative AI allowing cybercriminals to perform more sophisticated cyberattacks. Our laws need to be updated to meet these evolving threats and the needs of consumers. To accomplish this, our office recommends legislators consider the following proposals:

a. Reduce the notification deadline to three days

In 2018, our state experienced a then all-time high for data breach notices - just over 3.5 million. A few years later, in 2021, that record nearly doubled with just over 6.5 million notifications arriving in Washingtonians' mailboxes. And now, in 2024, our agency witnessed yet another record high, surpassing more than 11.6 million notifications to Washingtonians, which is greater than the total population of our state. These are staggering numbers.

Worse yet, not only are data breaches growing in frequency, but with the exponential growth in the use and sophistication of AI, and generative AI in particular, the magnitude of the threat of data breaches to people's privacy and safety has never been greater.[3]

In light of these growing threats, it is critical that individuals are aware of the compromise of their personal information as quickly as possible. This is not simply a matter of convenience, but one with implications for a person's physical and financial safety and wellbeing, as well as their dignity.[4] In a world where technology allows imitation of loved ones' voices, use of geolocation to identify homes and places of work, and other potentially nefarious acts at a massive scale in a short period of time, asking Washingtonians to wait up to a month for such critical information is unacceptable.[5,6]

While we do not have a lot of recent data regarding the impacts to Washingtonians specifically, a 2011 study of data breach notification laws suggests, "that losses are 21% lower when consumers detect identity theft within the first week, and 65% lower when consumers detect the crime within a year."[7] Furthermore, a 2006 survey prepared for the Federal Trade Commission (FTC) found that 30% of consumers, "who discovered that their personal information was being misused 6 months or more after it started had to spend $1,000 or more [in losses], compared to 10% of those who found the misuse within 6 months."[8] This same survey also found that 69% of consumers that discovered identity theft in six months or fewer resolved their problems in ten hours or less. That rate drops significantly, to 32%, for consumers who took more than six months to discover their identity had been stolen. A 2018 Bureau of Justice Statistics survey suggests that the incidence of consumers experiencing severe emotional distress doubles after spending more than one day working to resolve identity theft and escalates up to one in ten when the theft takes more than a week to resolve.[9] This evidence suggests informing consumers sooner can reduce the window that cybercriminals have to misuse stolen information, saving victims significant time, money, and peace of mind.

Under current law, Washingtonians must be notified within 30 days of discovering a breach, but 30 days allows too much potential for harm to consumers. Requiring data controllers to provide notice in a shorter time frame is not an unreasonable request. Since 2016, organizations subject to the European Union's (EU) General Data Protection Regulation (GDPR) – including those in the U.S. that offer goods or services to individuals in the EU – have operated under a much shorter deadline, with notification to a supervisory authority required within 72 hours of a breach's discovery.[10] Additionally, last April the U.S. Department of Homeland Security's

Cybersecurity and Infrastructure Security Agency (CISA) published a Notice of Proposed Rulemaking containing proposed rules to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Under CIRCIA, "covered entities" would be required to provide notice of a "cyber incident" to CISA within 72 hours and notice of a ransom payment within 24 hours.[11] Public comment on CIRCIA closed on July 3, 2024, and CISA is currently in the process of preparing a final rule for publication.

To address the urgency of the threat, the Legislature must reduce the deadline for data breach notifications to three days. This would make Washington the first state in the country with a three-day deadline and reiterate our state's commitment to cybersecurity and consumer protection.[12]

b. Create language access requirements for data breach notifications

According to the Office of Financial Management (OFM), 20% of households in Washington State speak a language other than English.[13] English is spoken less than "very well" in 7.9% of Washington households. Despite this, breached entities are not required to provide notice in a language other than English.

Example of data breach notice providing language assistance services, Change Healthcare Inc. (Aug. 3, 2024)

ATTENTION: If you speak English, language assistance services, free of charge, are available to you. Call 1-866-262-5342 (TTY: 1-866-262-5342).

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 1-866-262-5342 (TTY: 1-866-262-5342).

ATANSYON: Si w pale Kreyòl Ayisyen, gen sèvis èd pou lang ki disponib gratis pou ou. Rele 1-866-262-5342 (TTY: 1-866-262-5342)

CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số 11-866-262-5342 (TTY: 1-866-262-5342).

ATENÇÃO: Se fala português, encontram-se disponíveis serviços linguísticos, grátis. Ligue para 1-866-262-5342 (TTY: 1-866-262-5342).

注意:如果您使用繁體中文，您可以免費獲得語言援助服務。請致電 1-866-262-5342 (TTY: 1-866-262-5342)。

Affected residents who do not receive information about risks to their data are less likely to be able to take the steps necessary to protect themselves and their information. It is imperative that all Washingtonians have an opportunity to receive notice in their native language. In order to address this inequity, the Legislature should consider amending RCW 19.255 and RCW 42.56.590 to require breached entities to provide language accessibility options to impacted consumers, such as providing a phone number for an individual to call to speak with an interpreter or to request a translated version of the notice via text or email, at no cost to the consumer.

c. Expand the definition of "personal information" in RCW 19.255.005 to include:

i. Full name in combination with a redacted SSN that still exposes the last four digits of the number, bringing it into alignment with RCW 42.56.590; and

ii. Individual Tax Identification Numbers (ITINs).

In 2020, the Legislature passed SB 6187 expanding the definition of "personal information" to cover the combination of name and the last four digits of SSNs for breaches of a government agency. However, this amendment was not extended to breaches of businesses.[14] The Legislature should bring the definitions into alignment and provide consumers with more robust protections.

The Internal Revenue Service assigns ITINs to foreign-born individuals who are unable to acquire a SSN for the purposes of processing various tax-related documents. In other words, they are a unique identifier equivalent in sensitivity to a SSN. At present, ten states include ITINs in their definition of "personal information."[15]

In 2021, Washington State was home to just over 1.1 million foreign-born individuals, representing approximately 15% of the state's population.[16] All Washingtonians deserve the same protection for their sensitive data, regardless of whether they have SSNs or ITINs.

2. Require businesses to recognize and honor opt-out preference signals

An opt-out preference signal, also sometimes referred to as a "Global Opt-Out," is a browser setting that, when enabled, automatically sends a signal to any website the consumer visits that they are requesting to opt-out of the business's sharing or sale of their personal information.

Opt-out preference signals are already in use around the world, such as the Global Privacy Control (GPC).[17] The GPC allows consumers to make a single opt-out request, by enabling the GPC in their browser, which applies to any and all websites they visit. Businesses in Washington are not required to honor these consumer requests. When businesses do honor these preference signals, they give consumers the power to efficiently assert their data sharing preferences. Without them, consumers are unfairly burdened with the task of manually opting out of every single website they visit, and every service used by those websites or subsidiary owned by those entities' parent companies, to request their information not be processed, shared, or sold.

Colorado's data privacy law, the Colorado Privacy Act (CPA), which went into effect in July 2023, includes a requirement that businesses covered by the law must treat consumer opt-out signals as a valid request to opt-out of the sharing and sale of their personal information.[18] This provision went into effect on July 1, 2024. The Colorado State Department of Law (Attorney General's Office) released an approved public list of global opt-out signals.[19] Failure to honor these requests is subject to fines under the Colorado Consumer Protection Act, which can range from $2,000 to $20,000 for each violation.

If Washington's lawmakers require businesses to honor opt-out signals, Washingtonians will have greater control over their data, potentially reducing the impact of future data breaches.

3. Require transparency from data brokers and data collectors

Data brokers are businesses that specialize in collecting, aggregating, and selling consumer data. These firms often gather information from a range of sources, including public records, online activities, and purchase histories. This collected data is processed and repackaged into individual consumer profiles. These profiles can include information about an individual's demographic information, physical location, past purchases, websites visited, apps used, or even the content they consume online (e.g. YouTube channel subscriptions). These profiles are then sold to other businesses for a variety of purposes, including targeted advertising, credit scoring, and market research.

To better protect consumers, lawmakers should consider legislation to require data brokers and controllers

to report annually to individual consumers, via physical or electronic mail, what information they presently hold, what information they have shared or sold and to whom, in language that is clear and accessible.

Additionally, lawmakers should require data brokers to:

a. Register and obtain a license with the state and subject themself to oversight, such as providing regulators with information about the sources of their data, the type of data they collect, how it is processed, who they sell it to, and for what purposes;[20]

b. Have strict data security measures (e.g. data security incident response team, ransomware prevention measures, etc.) in place before they can register with the state;

c. Publicly disclose their policies for allowing consumers to opt-out of data processing; and

d. Pay a significant fine and incur suspension of their data broker license for violations of the above regulations.[21]

State Data Broker Registration Laws

	Year Implemented	Registration Fee	Regulating Body	Renewal Period	Penalties
Vermont	2018	$100	Secretary of State	Annual	$50 per day (max $10K per year)
California	2019	$400	California Privacy Protection Agency	Annual	$200 per day
Oregon	2023	$600	Dept. of Consumer and Business Services	Annual	$500 per day (max $10K per year)
Texas	2023	$300	Secretary of State	Annual	$100 per day (max $10K per year)

Currently, four states have Data Broker registration laws: California, Oregon, Texas, and Vermont. California's law requires brokers to register annually, pay a required $400 fee, and provide detailed information about their data collection and processing activities. Brokers also must agree to undergo independent audits every three years to ensure compliance.[22] Vermont's law imposes cybersecurity requirements on brokers, including maintaining a "comprehensive information security program."[23]

During our state's 2024 Legislative Session, HB 1799 was introduced in the House Committee on Consumer Protection & Business.[24] HB 1799 proposes that the Department of Licensing (DOL) oversee a data breach registry, which would require brokers to register and pay a fee set by DOL on an annual basis. HB 1799 does not include any language regarding audits or cybersecurity requirements. Were these additional regulations to be added to this language, additional work may be needed to determine if DOL is still the appropriate home for this work.

4. Consult with Tribes on how best to support their efforts in combatting cyberattacks

At present there are very few studies or publicly available information describing how data breaches affect various communities. This includes Tribes, which across the country have seen a significant increase in cybersecurity incidents over the last few years. One source indicates that cyberattacks against Tribes increased by nearly 60% in 2023. In the spring of 2024, both the Nisqually Red Wind Casino and Swinomish Casino and Lodge were hit with cyberattacks that forced both businesses to temporarily shut down. According to the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), Tribes across the country have been subjected to ransomware and other forms of cyberattacks that have, "...impacted network and email access, communications and social services infrastructure, economic enterprises [and in] some cases, these attacks have caused millions of dollars in losses."

Data breaches and cyberattacks aimed at Tribes and Tribal entities are simply a new form of extraction that harms Tribal members and Tribal sovereignty. To better understand the unique challenges that Tribes in our state face with regard to cybersecurity and data breaches, and the resources they need to respond, policymakers should consult with Washington Tribes to learn about what support would be beneficial for their efforts to combat the rise in cyberattacks on their communities.

Resources for Individuals Affected by a Data Breach or Identity Theft

First Steps

If you receive notice that your personal information was involved in a data breach, consider taking these two important steps:

1 Place a fraud alert and security freeze on your credit reports.

You can place a fraud alert with one phone call to one of the three major credit bureaus. This will prevent cyber criminals from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts, and all three will send you credit reports free of charge. Review the reports carefully for accounts you did not open, debts you cannot explain, or inaccurate information.

Visit our Credit Freeze & Fraud Alerts page for more information on how to place an alert or freeze: https://www.atg.wa.gov/credit-freeze-fraud-alerts.

2 Monitor your financial accounts, billing statements, and credit reports for any suspicious activity.

You may request a free annual credit report from each of the major nationwide credit bureaus at bureaus at www.annualcreditreport.com or call 1-877-322-8228.

Mitigating Identity Theft

Our office has information to help you mitigate your risk of identity theft. Much of this information also applies to mitigating your risk of a data breach. View our Protecting Personal Information Page for more information: https://www.atg.wa.gov/protecting-personal-information.

Additionally, if you receive notice that your data was exposed in a data breach, and you suspect your identity may have been stolen as a result, consider consulting the AGO's guide on recovering from identity theft: https://www.atg.wa.gov/recovering-identity-theft-or-fraud.

You can also report your situation directly to the Federal Trade Commission (FTC) online at identitytheft.gov. This website will record your report and offer tools to help you develop and execute a personal recovery plan.

Additionally, you can report your situation to your local police department and ask businesses to provide you with information about suspicious transactions made in your name. Download a template letter you can complete and send to businesses to request records, here: https://www.atg.wa.gov/db-letter.

Resources for Businesses and Agencies

Any organization entrusted with individuals' information is potentially susceptible to a data breach. The Attorney General's Office provides the following resources to help inform businesses on steps to secure the data they hold and protect it from being breached.

For additional information on data breach notification laws and requirements, visit our page on Washington's Data Breach Notification Laws: https://www.atg.wa.gov/washington-s-data-breach-notification-laws.

Protecting Consumers' Data

Below are basic steps for businesses to protect consumers' personal information:

- Understand your business's needs and how they relate to data security. This includes knowing what information you collect about consumers or clients, and knowing what information you retain and how it is retained.
- Consider identifying if the data you hold is subject to the definition of personal information under RCW 19.255.
- Minimize the amount of information that you collect and retain. Collect only information necessary to meet your business needs. Delete any information that is no longer necessary. Consider reviewing RCW 19.215, "Disposal of Personal Information" for more details.
- Develop policies for the collection, encryption, and use of personal information.
- Create and implement an information security plan, including an action plan for steps to take in the event of a data breach. This could include developing a dedicated Incident Response Team or implementing automated security technologies to detect attempted breaches.

External Resources

- FTC's "Protecting Personal Information: A Guide for Business"
  - This guide provides more in-depth information on the basic steps outlined above for protecting consumers' data.
- FTC's "Data Breach Response: A Guide for Business"
  - This guide provides critical information detailing what a business should do upon learning that their data security systems have been breached.
- FTC's "Privacy and Security" webpage
  - This webpage provides valuable information about existing federal data privacy laws, including additional resources for businesses.
- National Institute of Science and Technology (NIST) National Cybersecurity Center of Excellence: Security Guidance
  - This webpage provides information to help improve the cybersecurity of entities across many sectors.
- Better Business Bureau's Cybersecurity HQ
  - This webpage contains business education resources for small and midsize businesses to help them manage cybersecurity risks and learn about best practices.
- Internet Crime Complaint Center (IC3)
  - Internet Crime Complaint Center is the nation's central hub for reporting cybercrime. It also provides resources, such as industry alerts, to help keep businesses aware of recent cybercrime trends.
- Cybersecurity & Infrastructure Security Agency's "I've Been Hit by Ransomware!" guide
  - This guide provides step-by-step instructions for businesses to take after being hit with a ransomware attack.
- Cyber Readiness Institute's Ransomware Playbook
  - This guide provides businesses with information on how to prepare for, respond to, and recover from ransomware attacks.
- Cybersecurity & Infrastructure Security Agency's Tribal Affairs Webpage
  - This webpage provides resources and tools to assist Native American and Alaska Native Tribes in strengthening their cybersecurity infrastructure.

Data Analysis Methodology and Limitations

In assessing data breach notification data, it is important to acknowledge the nature and limitations of collecting and analyzing this information.

Data breaches are a moving target. Notices to the AGO are often sent with incomplete information that can be updated with new facts months after an initial notice. Resolving and understanding data breaches is complicated and time intensive. This is particularly true if the breached organization does not have a dedicated cybersecurity team on staff and, consequently, must seek external assistance on its analysis and containment measures. As such, it is important to keep in mind that the data provided in this report is a point-in-time snapshot of what we currently know. Put simply, the statistics in this report are estimates. The data in this year's report is a snapshot of what we know as of October 1, 2024.

In 2021, our office built a new data collection system for data breach notices, as well as a standardized online web form for breached organizations to provide notice to the AGO. Since implementation, this form has led to improved accuracy and completeness of notices regarding data breaches affecting Washingtonians, as well as a more efficient process for everyone involved. We hope more organizations will utilize this process going forward. This web form is available at: https://fortress.wa.gov/atg/formhandler/ago/databreachnotificationform.aspx.

Additionally, this database, which automatically updates as new information is added, provides our office a powerful tool for auditing and updating past years' data. As such, the AGO has revised several statistics reported in past years with more complete and accurate information. Of particular note, the total number of Washingtonians affected in 2023 increased from the 4.06 million figure we reported last October to an updated total of 4.52 million.

Lastly, it is important that we clarify what this report means when we refer to the "Number of Washingtonians Affected." This statistic comes from the notices breached organizations provide to our office, which must include the total number of Washington residents the organization notified of its data breach. This figure is a sum of all the data breach notices sent to Washingtonians and may not necessarily reflect the exact number of individual Washingtonians impacted by data breaches in a given year. This is because multiple breaches can affect a single Washingtonian. In other words, it is possible for a single Washington resident to receive multiple data breach notices, and thus appear multiple times within our dataset. The fact that the "Number of Washingtonians Affected" in 2024 exceeds the state's population perfectly illustrates this point. However, because this is the single best indicator we have of estimating the numerical impact to residents of our state, we refer to it as the "Number of Washingtonians Affected."

Notes and Citations

1. Office of Financial Management. (2024, June 28). "Washington state tops 8 million residents in 2024." Accessed August 2024, from https://ofm.wa.gov/about/news/2024/06/washington-state-tops-8-million-residents-2024.

2. RCW 19.255.010, effective March 2020. https://app.leg.wa.gov/RCW/default.aspx?cite=19.255.010.

3. Axios. (2023, June 13). "Generative AI is making voice scams easier to believe." Accessed August 2024, from https://www.axios.com/2023/06/13/generative-ai-voice-scams-easier-identity-fraud.

4. NBC Chicago. (2023, November 13). "FBI warns criminals are using A.I. to manipulate pictures and videos into explicit content." Accessed August 2024, from https://www.nbcchicago.com/news/local/fbi-warns-criminals-are-using-a-i-to-manipulate-pictures-and-videos-into-explicit-content/3260414/.

5. Trend Micro. (2023, June 28). "Virtual Kidnapping." Accessed August 2024, from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/how-cybercriminals-can-perform-virtual-kidnapping-scams-using-ai-voice-cloning-tools-and-chatgpt.

6. Fox News. (2023, May 30). "Who is watching you? AI can stalk unsuspecting victims with 'ease and precision': experts." Accessed August 2024, from https://www.foxnews.com/us/who-is-watching-you-ai-can-stalk-unsuspecting-victims-ease-precision-experts.

7. Romanosky, S., Telang, R., and Acquisti, A., (2011). "Do Data Breach Disclosure Laws Reduce Identity Theft?" *Journal of Policy Analysis and Management, Vol. 30* (No. 2), pp. 256-286. Accessed August 2024, from https://www.heinz.cmu.edu/~acquisti/papers/RomanoskyTelangAcquisti-JPAM-2011.pdf.

8. Federal Trade Commission. (2007, November). "2006 Identity Theft Survey Report." Accessed August 2024, from https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-2006-identity-theft-survey-report-prepared-commission-synovate/synovatereport.pdf.

9. U.S. Department of Justice. (2021, April). "Victims of Identity Theft, 2018." Accessed August 2024, from https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.

10. General Data Protection Regulation Art. 33, "Notification of a personal data breach to the supervisory authority." https://gdpr-info.eu/art-33-gdpr/.

11. Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 89 FR 23644 (proposed April 4, 2024) (to be codified at 6 CFR § 226). https://www.federalregister.gov/d/2024-06526/p-252.

12. The next closest deadline for consumer notice, were Washington to pass a three-day deadline, would be 30 days (CO, FL, ME). However, it is worth noting that Vermont requires notice to the Attorney General within 14 days and Puerto Rico requires notice to the Department of Consumer Affairs within ten days.

13. Office of Financial Management. (2024, July 9). "Language spoken at home." Accessed August 2024, from https://ofm.wa.gov/washington-data-research/statewide-data/washington-trends/social-economic-conditions/language-spoken-home.

14. No other state includes redacted Social Security Numbers (SSN) in their definition of Personal Information. The only other state that does something different than name in combination with SSN is Indiana, where breaching an SSN by itself triggers their law (no name needed).

15. Alabama, Arizona, California, Connecticut, Delaware, Maryland, Montana, North Carolina, Vermont, Wyoming.

16. OFM Health Care Research Center. (2023). "Washington state's immigrant population: 2010-21." Accessed August 2024, from https://ofm.wa.gov/sites/default/files/public/dataresearch/researchbriefs/brief110.pdf.

17. Global Privacy Control. Accessed October 2022, from https://globalprivacycontrol.org/.

18. Colorado Revised Statutes, Title 6, Article 1, Part 13, 6-1-1306 (1)(a)(IV). https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf.

19. Colorado Attorney General. "Universal Opt-Out Shortlist". Accessed June 2024, from https://coag.gov/uoom/.

20. In California, data broker registration goes through the Attorney General's Office: https://oag.ca.gov/data-broker/register. In Vermont, registration goes through the Secretary of State: https://sos.vermont.gov/corporations/other-services/data-brokers/.

21. The General Data Protection Regulation (GDPR) allows each member state's data regulator to fine violators up to 4% of global annual revenues of the preceding year or 20 million euros, whichever is higher. For any potential Washington data broker law, defining a fine as a percentage is recommended so that it scales with inflation over time.

22. California Privacy Protection Agency. "Information for Data Brokers." Accessed September 2024, from https://cppa.ca.gov/data_brokers/.

23. Vermont Statutes Annotated, Title 9, Chapter 062, Subchapter 005, § 2447 (a)(2). https://legislature.vermont.gov/statutes/section/09/062/02447.

24. HB 1799, introduced January 8, 2024. https://app.leg.wa.gov/billsummary?BillNumber=1799&Initiative=false&Year=2023.