Duchelle Nunes

DataBytes  Privacy-Technologies-for-Financial-Intelligence

Equifax Data Sharing Report

Contents

[Introduction 2](#_Toc153125905)

[The two main ways how Equifax collects the personal information in Australia are: 3](#_Toc153125906)

[Equifax collects, holds, uses, and discloses personal information for various purposes across its different businesses Source 4](#_Toc153125907)

[The Equifax 2017 Data Breach: 5](#_Toc153125908)

[Additional links on Apache Struts2 Vulnerability and Equifax Hack 5](#_Toc153125909)

[Data Sharing Practices at Equifax 6](#_Toc153125910)

[Potential Risks and Implications of Data Sharing 6](#_Toc153125911)

[Recommendations for Mitigating Risks and Enhancing Data Privacy 7](#_Toc153125912)

[Data Security: 7](#_Toc153125913)

[Data Privacy: 7](#_Toc153125914)

[Data Integrity and Availability: 7](#_Toc153125915)

[Data Access Control: 7](#_Toc153125916)

[Conclusion 7](#_Toc153125917)

[Reference 9](#_Toc153125918)

# Introduction

**What is credit reporting?**

According to oaic.gov.au (2023), In Australia Credit reporting helps keep the customers personal information safe while also letting lenders know how responsible the customers are with their credit, like loans. It balances the privacy with the lender's need to assess the financial situation. This includes credit providers, reporting agencies, and others like mortgage insurers. Special laws in Australia govern how these organizations handle the customers credit information.

**How credit reporting works:**

* Lenders share the customers credit information: When the customers borrow money, the lender reports the customers payment history to the credit bureaus.
* Credit bureaus build the customers report: These bureaus collect and store the customers credit information, creating a report that shows the customers creditworthiness.
* Lenders use the customers report: When the customers apply for a loan or credit card, lenders check the customers report to decide whether to approve the customers.
* Sharing information: In some cases, lenders can share the customers credit information with other lenders or third parties, but only under specific rules.
* Regulated information: Credit bureaus may also share certain information with external dispute resolution bodies or enforcement agencies.

|  |  |
| --- | --- |
|  |  |

Source: oaic.gov.au (2023)

The Equifax group of companies in Australia (formerly the Veda group of companies) is one of the top three credit bureaus in the US and one of the top few in Australia. They play a crucial role in the financial system by collecting and analysing individual credit information. The primary business of Equifax is the assimilation of financial records-based information, this information is then sold to creditors, who use it to assess creditworthiness and make informed decisions about granting loans. It is important to note, Equifax doesn't directly decide loan approvals, but rather serves as a provider of credit reports and scores, which are key indicators of an individual's financial responsibility and predict their ability to repay debts. These scores however heavily influence loan eligibility and interest rates, making Equifax a vital player in shaping financial opportunities for individuals (Schmitt, 2021).

According to the company website, Equifax operates several businesses in Australia and New Zealand, offering various services across credit reporting, tenancy, HR solutions, risk assessment, marketing, and personal solutions (Equifax, 2023a).

**These include:**

* **Credit Reporting:** Equifax Information Services and Solutions (EISS) handles credit reporting in Australia, and Equifax New Zealand Information Services and Solutions Limited in New Zealand.
* **Tenancy:** National Tenancy Database, managed by EISS, provides a tenancy database for real estate agents.
* **HR Solutions:** Equifax offers various HR services through fit2work (background screening), Equifax Human Resources Platform (onboarding & management), eCredential (clinical credentialing), and Verification Exchange™ (employment verification).
* **Marketing & Personal Solutions:** Equifax Australia Marketing Services and Equifax Australia Personal Solutions provide marketing services and communication channels for Equifax and their clients.
* **Risk Assessment:** Equifax Australasia Credit Ratings and Kingsway Financial Assessments offer risk assessment services for suppliers and contractors.
* **Income Verification:** Equifax Australia Commercial Services and Solutions provides income and expenditure verification services through MOGOplus and Tenant Affordability Check.

Equifax gathers the personal information in Australia primarily from third parties, depending on the purpose for collection. These sources include real estate agents, utility providers, legal professionals, lenders, government agencies, and more. In specific situations, Equifax also collects information directly from the customers, such as when they apply for certain services, request credit reports, or contact them regarding marketing or tenancy information.

## The two main ways how Equifax collects the personal information in Australia are:

### Third-Party Sources:

* Real estate agents and platforms provide information related to property purchases and rentals.
* Utility providers share information about the customers utility usage and payment history.
* Lawyers, insurers, and other financial institutions offer data relevant to legal proceedings, insurance claims, and financial transactions.
* Government agencies, like ASIC and the AEC, contribute information related to business activities and voter registration.
* Market Research & Direct Marketing: These entities provide consumer data for research and marketing purposes.
* Other Sources: Service providers, external dispute resolution schemes, and related companies may also share relevant information.

### Direct Collection from the customer:

* Secure Sentinel & Identity Watch: Membership applications and activity data are collected.
* Credit Reports: Information is gathered when you request the customers credit report or dispute information.
* Data-driven Marketing: Contacting Data-driven Marketing regarding marketing materials triggers data collection.
* NTD Tenancy Database: Information is collected when requesting a copy of the customers tenancy file or requesting amendments.
* Employment Verification: Providing information for background checks leads to data collection.
* Carhistory.com.au: Personal information is collected when accessing information through this website.
* Marketing Opt-in: Choosing to receive offers and product information from Equifax allows them to store the customers details.
* MOGOplus & Tenant Affordability Check: These applications collect personal information and, in the case of MOGOplus, information from Centrelink about government assistance.
* Employee/Contractor Applications: Information is collected during the application process for employment or contractor roles.
* Direct Communication: Providing information through websites, representatives, or other channels allows Equifax to collect data.

Source (Equifax, 2023b)

## Equifax: A Breakdown of Data Use Across Businesses

Equifax collects, holds, uses, and discloses personal information for various purposes across its different businesses Source (Equifax, 2023c) This can be categorised into:

### Consumer Risk & Identity:

* Identity Solutions: Verify identity for AML/CTF, fraud detection, and collection services.
* Employment Verification: Verify background of candidates and employees.
* MOGOplus and Tenant Affordability Check: Verify income and affordability for financial institutions and landlords.

### Commercial Risk & Information Services:

* Provide commercial credit reports to credit providers, trade credit providers, and others.

### B2C Marketing Services:

* Equifax Score, My Credit File, Secure Sentinel, Identity Watch, carhistory.com.au, NTD: Provide credit scoring, identity theft protection, and other services to consumers.
* ReduceMyBills.com.au: Assist consumers in finding better deals on energy, phone, internet, and pay TV services.
* Tenancycheck.com.au: Allow landlords to verify tenant information.

### Equifax HR Solutions:

* To manage HR platforms and provide workforce data management services.

### Veda Group Pty Limited (former shareholder information):

* To process shareholder applications, service shareholder needs, and communicate with shareholders.

The Equifax 2017 Data Breach:

According to Krebs (2017) Equifax's 2017 data breach involved over 200,000 stolen credit cards. This prompted Visa and MasterCard to send alerts to financial institutions regarding these compromised cards, with dates ranging from November 2016 to July 2017. However, Krebs (2017) article suggests that Equifax claims the data was downloaded in one instance during mid-May 2017. The company denies the presence of any credit card harvesting malware and maintains the access only occurred after mid-May 2017.

Krebs (2017) suggest that further investigation revealed that the breach stemmed from a vulnerability in Apache Struts software, disclosed in March 2017. While a patch was available, Equifax's system remained unpatched for four months, allowing hackers to exploit the vulnerability.

The article, Krebs (2017) provides details about the vulnerability, its discovery, and its exploitability. It also highlights the discrepancy between the dates provided by Visa/MasterCard and Equifax's statement. The stolen data included credit card numbers, expiration dates, and cardholder names. Additionally, Visa later clarified that the stolen records also likely contained Social Security numbers and addresses. This suggests the data belonged to individuals signing up for Equifax's credit monitoring services. Overall, the article emphasises the seriousness of the Equifax data breach and raises questions about the company's security practices and timeline of events.

## Additional links on Apache Struts2 Vulnerability and Equifax Hack

Apache Struts2 Remote Code Execution Vulnerability (CVE-2023-50164): <https://twitter.com/theapachestruts?lang=en>

Apache Struts2 Double OGNL Evaluation Vulnerability (CVE-2020-17530): <https://threatprotect.qualys.com/2020/08/17/apache-struts-2-remote-code-execution-vulnerability-cve-2019-0230-cve-2019-0233/>

Apache Struts : Security vulnerabilities, CVEs: <https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-6117/Apache-Struts.html>

Apache Struts 2 Multiple Vulnerabilities: <https://www.hkcert.org/>

How critical is the Apache Struts2 Vulnerability??: <https://medium.com/@abhishekY495/rce-via-apache-struts2-still-out-there-b15ce205aa21>

**Other Articles:**

Apache Struts 2: how technical and development gaps caused the Equifax Breach: <https://www.researchgate.net/publication/337289678_Fixing_of_Security_Vulnerabilities_in_Open_Source_Projects_A_Case_Study_of_Apache_HTTP_Server_and_Apache_Tomcat>

Equifax, Apache Struts, and CVE-2017-5638 Vulnerability: <https://userapps.support.sap.com/sap/support/knowledge/en/3194035>

**Additional Resources:**

Apache Struts 2 Security Documentation: <https://struts.apache.org/security/>

Apache Struts 2 OGNL Expression Evaluation: <https://struts.apache.org/tag-developers/ognl>

OWASP Struts 2 Cheat Sheet: <https://cyberscoop.com/owasp-top-10-2017/>

Snyk Struts 2 Vulnerability Database: <https://security.snyk.io/package/maven/org.apache.struts%3Astruts2-core>

# Data Sharing Practices at Equifax

According to Swati Khandelwal (2017) The massive 2017 Equifax data breach, impacted 143 million individuals and was attributed to an unpatched vulnerability in the widely used Apache Struts software. The article suggests that this vulnerability, CVE-2017-5638, rated critical with a severity score of 10.0, was disclosed and addressed by Apache two months before the breach. However, Equifax failed to apply the available patches, leaving their systems susceptible to attack.

Exploiting this remote code execution flaw in the Jakarta Multipart parser, hackers successfully installed malicious applications on Equifax's servers, enabling them to access and steal sensitive personal data (Khandelwal, 2017). This highlights the critical need for companies to prioritize patching known vulnerabilities promptly, which Equifax failed to do as part of that business practices.

Following the breach, Equifax offered free credit monitoring and identity theft protection services to affected individuals. While the company initially faced criticism for its security measures, they implemented improvements and continue to work with law enforcement to address the incident. Khandelwal (2017) emphasises that the case of data sharing practices at Equifax in 2017, serves as a stark reminder of the potential consequences of failing to address cybersecurity vulnerabilities and the importance of proactive defence against cyber threats.

# Potential Risks and Implications of Data Sharing

The article by bbc.com (2017) emphasises the extensive data sharing practices of Equifax and other credit bureaus raise significant concerns regarding the potential risks and implications for consumers. These concerns fall into the below key categories:

**Identity Theft and Fraud:** The exposure of personal information, including social security numbers and credit card details, creates a heightened risk of identity theft and financial fraud. This can have devastating consequences for individuals, including financial losses, damage to credit scores, and emotional distress.

**Erosion of Privacy:** The vast amount of data collected by credit bureaus paints an intimate picture of individuals' lives, including their financial history, employment status, and even purchasing habits. This raises concerns about the erosion of privacy and the potential for data misuse or exploitation.

**Algorithmic Bias:** Credit scoring algorithms, which rely on data collected by credit bureaus, can perpetuate and amplify existing biases against certain groups of individuals. This can lead to unfair credit decisions and limit access to financial opportunities for specific demographics.

**Data Security Breaches:** The large-scale data breaches experienced by Equifax and other credit bureaus highlight the vulnerability of sensitive information. These breaches expose consumers to identity theft, financial fraud, and other harms.

**Lack of Transparency and Control:** Consumers often lack transparency regarding how their data is collected, used, and shared by credit bureaus. This lack of control and understanding can lead to customers feeling exploited and hesitant to trust companies with the financial data.

# Recommendations for Mitigating Risks and Enhancing Data Privacy

According to Velumadhava and Selvamani (2015) Companies can do work in the below areas to protect the customers privacy.

### Data Security:

* Encryption at rest and in transit: Companies should utilise industry-standard algorithms to protect sensitive data throughout the lifecycle of the data.
* Data owner-controlled access: Companies can implement mechanisms that allow users to grant specific individuals or groups access to their data, minimizing exposure.
* Heterogeneous data security: Employ diverse security measures based on data type and sensitivity to provide granular protection.

### Data Privacy:

* Data minimisation: Companies should endeavour to collect and store only the data necessary for legitimate purposes, minimising potential harm in the event of a breach.
* Privacy-enhancing technologies (PETs): Leverage anonymisation, pseudonymisation, and other PETs to obfuscate data and reduce re-identification risks.
* Data protection as a service (DPaaS): Leverage cloud-based solutions to implement robust data protection measures and ensure compliance.

### Data Integrity and Availability:

* Data hashing: Companies should practice calculating the unique checksums for files before uploading to verify data integrity and prevent unauthorised modifications.
* RSA-based data integrity checks: Companies should combine RSA signatures with identity-based cryptography for enhanced data integrity assurance.
* Fine-grained access control: Companies should permit data processing without revealing full data contents, ensuring data availability while protecting privacy.

### Data Access Control:

* Distributed access control architecture: Companies must implement a decentralized system for managing data access, enhancing security and scalability.
* Attribute-based access control (ABAC): Utilize user attributes and data characteristics to grant access dynamically, ensuring finer control.
* Permission as a service (PaaS): Companies can also dynamically manage access permissions based on user roles and data sensitivity, providing a flexible solution.

# Conclusion

Equifax is one of the top credit bureaus in the US and Australia, responsible for collecting and analysing individual credit information. This information is used by lenders to assess creditworthiness and make informed decisions about granting loans. Equifax also offers various services such as tenancy databases, HR solutions, risk assessment, marketing, and personal solutions.

However, Equifax's data sharing practices have raised significant concerns regarding consumer privacy. The company's 2017 data breach exposed the sensitive data of 143 million individuals due to an unpatched vulnerability. This highlights the potential risks associated with large-scale data collection and sharing, including identity theft, fraud, and erosion of privacy.

To mitigate these risks and enhance data privacy, Equifax needed to implement several technical solutions. These can include encryption, data owner-controlled access, heterogeneous data security, data minimization, privacy-enhancing technologies, data protection as a service, data hashing, RSA-based data integrity checks, fine-grained access control, distributed access control architecture, attribute-based access control, and permission as a service.

Credit Bureaus along with Equifax also needed to prioritise responsible data sharing practices, ensuring transparency and control over how consumer data is used and shared. This requires ongoing scrutiny and evaluation of their activities, along with adherence to regulatory oversight and industry best practices.

# Reference

Equifax. (2023), ‘Who We Are’, Access date 7th December 2023, Link: <https://www.equifax.com/about-equifax/who-we-are/#:~:text=As%20a%20global%20data%2C%20analytics,commerce%2C%20and%20government%20agencies%2C%20make>

Equifax. (2023a), Privacy Policy (Australia), ‘Equifax comprises of a number of separate businesses’ , Access date 7th December 2023, Link: <https://www.equifax.com.au/privacy>

Equifax. (2023b), Privacy Policy (Australia), ‘How Equifax collects your personal information’ , Access date 7th December 2023, Link: <https://www.equifax.com.au/privacy>

Equifax. (2023c), Privacy Policy (Australia), ‘The kinds of, and purposes for which Equifax collects, holds, uses and discloses personal information’, Access date 7th December 2023, Link: <https://www.equifax.com.au/privacy>

Khandelwal, S. (2017), ‘Equifax Suffered Data Breach After It Failed to Patch Old Apache Struts Flaw’, Access date 7th December 2023, Link: <https://thehackernews.com/2017/09/equifax-apache-struts.html>

OAIC.gov.au (2023), ‘What is credit reporting?’, Access date 7th December 2023, Link:

<https://www.oaic.gov.au/privacy/your-privacy-rights/credit-reporting/what-is-credit-reporting>

Schmitt, K. (2021), ’Basics of What a Credit Bureau Is and Does, Plus Major Ones’, Access date 7th December 2023, Link: <https://www.investopedia.com/terms/c/creditbureau.asp>

"CVE-2017-5638 - Apache Struts2 S2-045 #8064". GitHub. March 7, 2017. Access date 7th December 2023, Link. <https://github.com/rapid7/metasploit-framework/issues/8064>

Krebs, B (2017), ‘Equifax Hackers Stole 200k Credit Card Accounts in One Fell Swoop’, vulners.com, Access date 7th December 2023, Link: <https://vulners.com/krebs/KREBS:EE70929DE902D9B233E209B73C1AD4A0>

Velumadhava, R & Selvamani, K (2015), ‘Data Security Challenges and Its Solutions in Cloud Computing’, Access date 7th December 2023, Link: <https://www.sciencedirect.com/science/article/pii/S1877050915006808>