USAA Web Audit Report

Dylan Ramdhan, Shangmin Chen, Michael Mei, Issac Chan

Oct 13, 2023

Technical Analysis

When conducting the technical analysis, we found many tracking cookies. Cookies are all from the same origin, usaa.com, but the tracking cookies use 3rd party data softwares. USAA uses Oracle's Maxymiser (mmapi) that expires in 1 year, LiveRamp(cjLiveRampLastCall) that expires in 1 year, Adobe's Experience Cloud ID (ECID, MemberECID) that expires at the end of the session, and Tealium's Utag (utag_main) that expires in 1 year [1, 2]. Maxymiser provides USAA with advanced website testing, real-time behavioral targeting, and in-session personalization. LiveRamp collects user data to improve the user experience. Experience Cloud ID is a way for USAA to identify user clients. Tealium's Utag is a javascript library USAA imported to organize data, it stores a unique ID, records timestamp when user visits the site, number of pages viewed and number of visits to site, it is implemented to optimize user experience. Other than LiveRamp's cookie, all other cookies mentioned above were not secure cookies. Some functional cookies are the ak_esd cookie and bm_sz cookie that is a secure location cookie and Akamai Bot Manager's anti-fraud and bot attack cookie respectively [2]. When exploring more in the element page, we found more about Oracle's Maxymiser, we found a mmapi javascript page in the usaa origin that we can paste into the search bar and have access to, to compromise the javascript source page can be dangerous [3]. When looking into the urls fetched, no potential malicious urls were fetched, mostly image files and svg files that belonged to the ussa origin. When looking into tracking pixels, we see that there was a hidden body on the top of the page that contained Google ad service [6]. The connection is HTTPS only, the connection is very secure [4]. When using the chrome HSTS tool, we found that USAA is indeed using HSTS, which is great as it prevents potential man in the middle attacks and protects SSL/TLS [5]. We moved on to find CSRF defenses, and were extremely surprised to find no CSRF defense at all, even when visiting the page with the login. There were no cookies or mentions in the elements/sources of chrome developer tools of a CSRF token. In terms of javascript libraries, we did not find anything that was outdated, everything was great. Lastly, when we looked into plugins, we found that the site had none, meaning the site does not have to worry about a potential attack by using outdated plugins.

Private Policy

Like many financial companies across the United States, USAA shares its similarities with securing personal information and its usage of its 'Private Policy'. When further investigating USAA's policy site, it becomes noticeable that many of its usages of personal data are within compliance and means of the federal law that is placed for the protection of user data. Much of this personal data is shared within the company and its affiliated companies, such as its

child company, the ‘Garrison Property and Casualty Insurance Company’. USAA continues to use personal data for daily business purposes as many companies today utilize this data for advertisement purposes. In the documentation that was provided within the ‘Private Policy’ we can see that a diagram demonstrates the usage of personal information that USAA utilizes that remains in compliance with federal law [5].

GDPR

The USAA’s privacy section of their website offers two primary sources that indicate GDPR compliance: The European Privacy Statement and the California Consumer Privacy Act (CCPA) Privacy Notice. GDPR requirements are in accordance with the GDPR principles. According to the GDPR requirements on their website, there are seven principles of GDPR: Lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

The European Privacy Statement (EPS) indicates the purpose of collecting users’ personal data via cookies; it states that the collection of data will be used for marketing purposes to enhance and personalize content for the users. The statement mentions the use of two general categories of cookies: session cookies and persistent cookies. The session cookie is a cookie that would be stored in the cookie file of the browser until it is closed and the persistent cookie is stored in the user’s hard drive until expiration or erasure. Third party web beacons are also mentioned to be used for optimization in online advertising.

The CCPA Privacy Notice is similar to the European Privacy Statement in many aspects in regards to demonstrating compliance with the seven principles of GDPR; however, there are slight differences as a product of government regulations and business practices. For instance, the CCPA Privacy Notice is comparatively more specific than the European statement, where the CCPA categorizes the data collected into eight categories compared to the EPS's four. Those eight categories include: Identifiers, Addition Data Subject to California Civil Code, Protected Classifications, Online Activity, Sensory Information, Employment Information, Education Information, and Inferences. The purpose of data collection via cookies are also slightly different, where the CCPA indicates the selling and sharing of personal data for business operations and legal compliance, whereas the EPS states that data will not be shared or sold to third parties; albeit the CCPA explicitly mentions the two types of data being sold or shared: Identifiers, such as names and addresses, and Internet or network activity information, such as browsing history and interactions with the website.

Login and Password Reset Flow

The USAA website has multiple login and account access options. When you click “Log On” on their main site, you are redirected to a page where you can determine if you’re new to USAA or already a member [7]. New users can click “Join USAA,” while existing members can

log in with a USAA ID and password. If you choose to join, you'll go through a series of questions to check your eligibility, including questions about military service and relatives' USAA memberships. If eligible, you can either call USAA or provide personal information to make the account. Another option would be to click "I need help logging on" which gives you 3 options – Recover Online ID, Reset Password, and Register for Digital Access. The first and second options would prompt you to enter one of the 3 – USAA numbers, SSN, or Tax ID number – along with one of the 3 – phone number, email, or government ID [8]. This is a more secure ID recovery and password reset process compared to other sites. The latter option, digital access registration, would assume user-proclaimed eligibility. The user will still go through screening before the account is officially made.

Potential Exploits

USAA employs Multi-factor-authentication. These processes include quick-logon, biometric screening, browser recognition, and CyberCode text or token. Quick-logon entails a one-time secure code that gets automatically added to the PIN. Biometric screening can pose a potential threat with companies that hold biometric data such as 23andMe being hacked. This method requires the same process as unlocking an iPhone with facial recognition or fingerprint. Browser recognition bypasses any other form of authentication. This option prompts the user with "Trust this device" or "Remember me for X amount of days?" Lastly CyberCode is USAA's PIN replacement authentication method which involves a one-time secure code that replaces the pre-existing user PIN. There are still risks with their "strongest authentication options". For their SMS-based MFA, such as the CyberCode Text and potentially the Quick-Logon, there could be a lack of encryption, network outage, SS7 attack, and SIM-Swapping which are all potential risks [10].

Conclusion

After auditing the USAA website, we found that the site maintains its compliance to both the Privacy Policy and GDPR policies, which means it manages user data within federal law compliance. Despite the secure HTTPS connections and its verifying robust MFA implemented, there lies existing inconsistencies in the implementation of security features which can be pointed out in both its CSRF defenses and SMS-based MFA. While the website is fundamentally secure, we find that there needs to be improvement in these areas as it is essential for enhancing the overall security of the USAA website.

Appendix

[1] Cookies using Chrome Web Dev Tools

Name	Value	Domain	Path	Expire…	Size	HttpO…	Secure	Same…	Partiti…	Prio…
s_pers	%20gpv_pn%3Dww…	.usaa.com	/	2023-…	149					Medium
bm_sz	9FE15C40022DCA93…	.usaa.com	/	2023-…	386					Medium
akusaa	akusaass7WsxbQgFa…	.usaa.com	/	2024-…	100		✓			Medium
cjLiveRampLastCall	2023-10-11T22:48:22…	.usaa.com	/	2024-…	42		✓			Medium
amlbcookie	01	.usaa.com	/	Session	12	✓	✓	None		Medium
_cls_s	948bf338-e3f2-4c2e-…	.usaa.com	/	Session	44		✓	None		Medium
MemberECID	d701fb21-b31b-4638…	.usaa.com	/	Session	46					Medium
cjConsent	MHxOfDB8Tnww	.usaa.com	/	2024-…	21		✓			Medium
_cls_v	8eebc496-8f47-4e9c-…	.usaa.com	/	2024-…	42		✓	None		Medium
ak_esd	US:MA	.usaa.com	/	Session	11		✓			Medium
s_sess	%20s_cc%3Dtrue%3B	.usaa.com	/	Session	23					Medium
_abck	5D07DB7F0D3B22D…	.usaa.com	/	2024-…	465		✓			Medium
utag_main	v_id:018af6b5a15f001…	.usaa.com	/	2024-…	276					Medium
cjUser	c18bfed2-3f03-477c-…	.usaa.com	/	2024-…	42		✓	None		Medium
MemberGlobalSession	2:1111:18lYY9DA532…	.usaa.com	/	Session	46		✓			Medium
ECID	d701fb21-b31b-4638…	.usaa.com	/	Session	40					Medium
JSESSIONID	000083xBXZlTbpwTi…	.usaa.com	/	Session	47	✓	✓			Medium
dcenveq	ea	.usaa.com	/	Session	9		✓			Medium
AMCV_47977B2A53A85221…	1585540135%7CMC…	.usaa.com	/	2024-…	133					Medium
dcenv	1a	.usaa.com	/	Session	7		✓			Medium
akmachineid	akma/tGxH6rFwGqcp…	.usaa.com	/	2024-…	103		✓			Medium

[2] Cookies using Safari Web Dev Tool

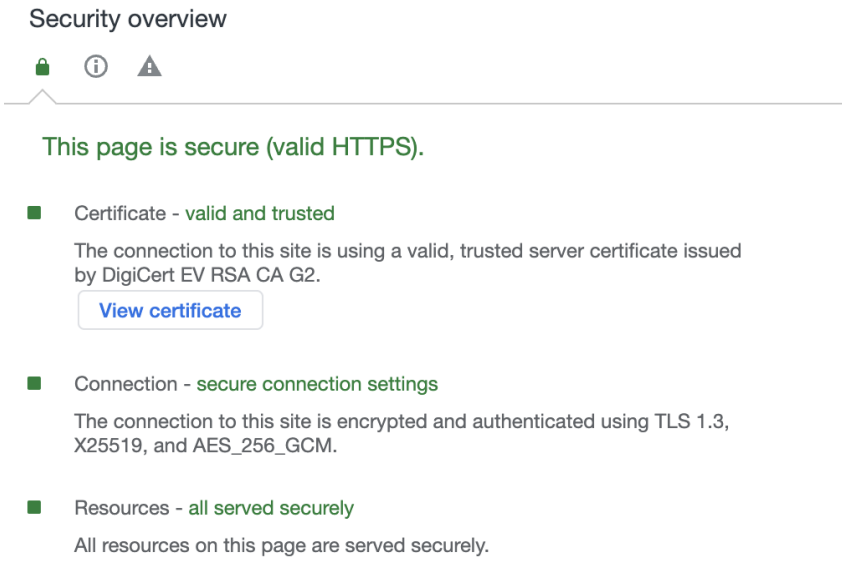
Name	Value	Domain	Path	Expires	Size	Secure	HttpOnly	S…
_abck	9CD6B03BA…	.usaa.com	/	10/12/2024, 1…	465…	✓		—
_cls_s	caf7d6b4-a9…	.usaa.com	/	Session	44 B	✓		—
_cls_v	9f1391cc-33…	.usaa.com	/	10/1/2028, 11…	42 B	✓		—
_fbp	fb.1.1696347…	.usaa.com	/	1/11/2024, 12:…	33 B			—
_gcl_au	1.1.21363678…	.usaa.com	/	1/1/2024, 10:…	32 B			—
_scid	e2496856-f…	.usaa.com	/	11/2/2024, 4:…	41 B			Lax
_scid_r	e2496856-f…	.usaa.com	/	11/12/2024, 4…	43 B			Lax
_screload		.usaa.com	/	Session	9 B			Lax
_sctr	1%7C169708…	.usaa.com	/	11/10/2024, 3…	22 B			Lax
ak_esd	US:MA	.usaa.com	/	Session	11 B	✓		—
akmachineid	akmajLd7tKl…	.usaa.com	/	9/30/2033, 1…	103 B	✓		—
akusaa	akusaaz1NeE…	.usaa.com	/	10/10/2033, 1…	100 B	✓		—
AMCV_47977B2A53A852210A49…	1585540135…	.usaa.com	/	10/3/2025, 11…	163 B			—
AMCVS_47977B2A53A852210A4…	1	.usaa.com	/	Session	42 B			—
amlbcookie	01	.usaa.com	/	Session	12 B	✓	✓	—
bm_sz	6E8D909F60…	.usaa.com	/	10/13/2023, …	354…			—
dcenv	2a	.usaa.com	/	Session	7 B	✓		—
dcenveq	ea	.usaa.com	/	Session	9 B	✓		—
ECID	6c474e6e-6…	.usaa.com	/	Session	40 B			—
JSESSIONID	0000mijNRh…	.usaa.com	/	Session	67 B	✓	✓	—
MemberECID	2|126665c2b…	.usaa.com	/	Session	76 B	✓		—
MemberGlobalSession	2:1101:7WSF…	.usaa.com	/	Session	47 B	✓		—
mmapi.e.loggedIn	true	.usaa.com	/	10/12/2024, 1…	20 B			—
mmapi.p.bid	%22prodphx…	.usaa.com	/	10/13/2023, 1…	30 B			—
mmapi.p.pd	%22eLWrDp…	.usaa.com	/	10/12/2024, 1…	307…			—
mmapi.p.srv	%22prodphx…	.usaa.com	/	10/12/2024, 1…	30 B			—
mmapi.p.uat	%7B%22S%…	.usaa.com	/	10/12/2024, 1…	79 B			—
s_pers	%20gpv_pn…	.usaa.com	/	11/12/2023, 1…	149 B			—
s_sess	%20s_cc%3…	.usaa.com	/	Session	23 B			—
utag_main	v_id:018af63…	.usaa.com	/	10/12/2024, 1…	276…			—

[3] MMCORE

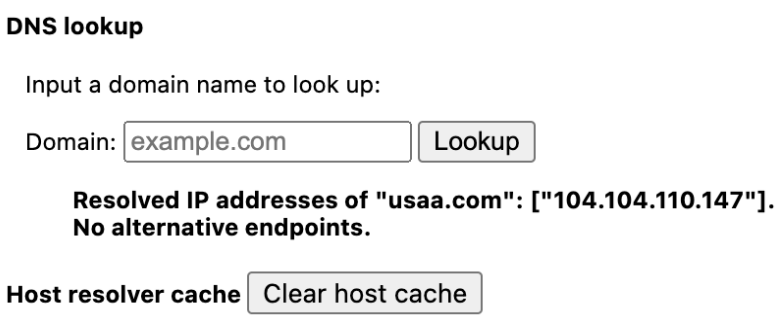
https://mvt.usaa.com/mvt/mmcore.js

```
19                  }
20  ~~~~~~~~~~~~~~~~~~
-     </script>
-     <script data-react-helmet="true" src="https://mvt.usaa.com/mvt/mmcore.js" type="text/javascript"></script>
-     <link rel="stylesheet" href="/my/public-home/ent-pubhome-app.46011712f5c43a66c790.css"/>
-   ead>
```

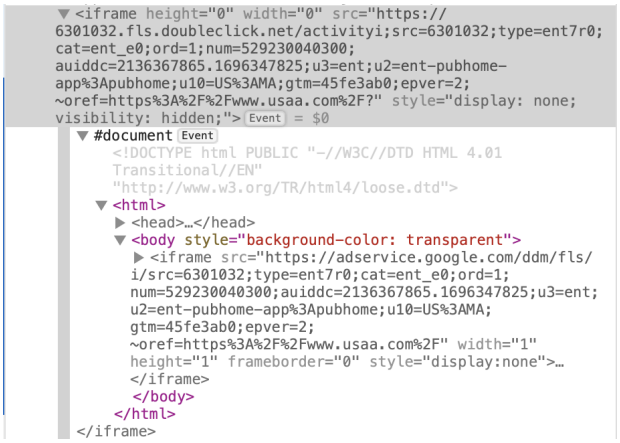
[4] Chrome Security Tab



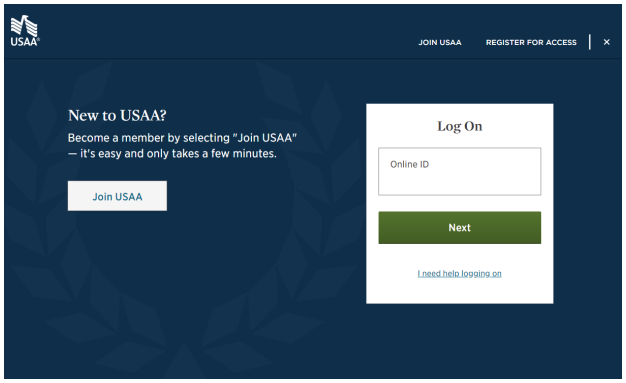
[5] HSTS chrome://net-internals/#hsts



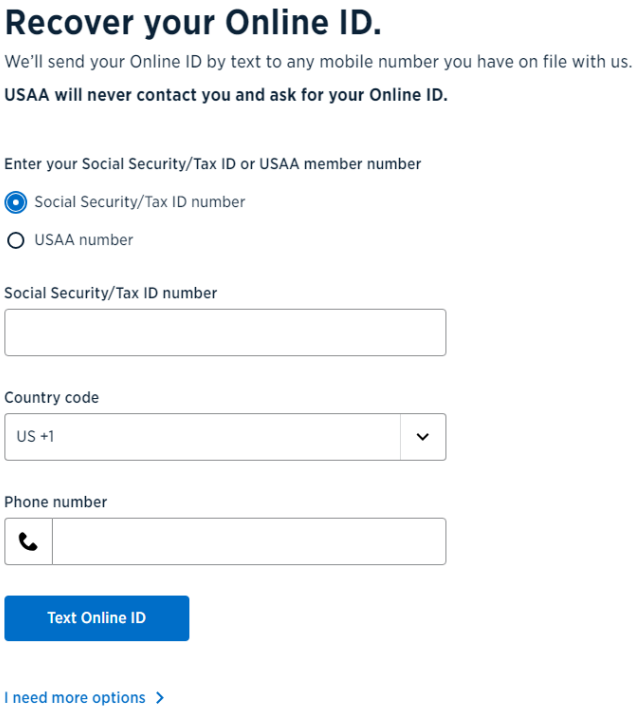
[6] Adservice Google iFrame (Safari)



[7] USAA main login page



[8] Requirements for Recovery/Reset



[9] Diagram of 'Reasons USAA Can Share Data'

Reasons we can share your personal information	Does USAA share?	Can you limit this sharing?
For our everyday business purposes — such as to process your transactions, maintain your accounts, respond to court orders and legal investigations, or report to credit bureaus	**Yes**	**No**
For our marketing purposes — to offer our products and services to you	**Yes**	**No**
For joint marketing with other financial companies	**No**	**We don't share**
For our affiliates' everyday business purposes — information about your transactions and experiences	**Yes**	**No**
For our affiliates' everyday business purposes — information about your creditworthiness	**Yes**	**Yes**
For our affiliates to market to you	**Yes**	**Yes**
For nonaffiliates to market to you	**No**	**We don't share**

[10] Source
https://cyberhoot.com/blog/top-five-risks-from-sms-based-mfa/#:~:text=SMS%2Dbased%20MFA%20has%20been%20a%20widely%20used%20method%20for,associated%20with%20SMS%2Dbased%20MFA