Tracking and Online Banking: A Survey

Dr. Sam Macbeth <sam@cliqz.com>

Cliqz GmbH, https://cliqz.com

August 1, 2016

1 Introduction

The proliferation of third-party tools for augmenting web pages and providing detailed intelligence and analytics to their owners has lead to a hidden layer in the Internet, where, when visiting one company's website, tens of other companies are invited to see who you are and what you are viewing [8, 3]. Which companies are third-parties in a website, and what data about you they are collecting, is only visible with special browser extensions [1, 4].

In adding a third-party service to their website, the website owner is bestowing trust in this third party. If a third-party Javascript file is loaded into the page, the third-party is given the ability to modify the page at will, intercept all user input on the page, as well as load any other scripts or third parties they wish. Loading third-party images in the page allows the third-party to know the page you're visiting, via the `Referer` header, your IP address, and may allow them to further track your browser via Cookies [2].

The decision of who to place this trust in is particularly acute in the case of online banking. This is an area which requires strong security in order to keep users' money and data safe. Furthermore, banking information is sensitive to many consumers, who will not want this shared with other companies without their permission.

To access how third-party services are being used in online-banking portals, we present a survey of German banks, analysing where third parties are included in online-banking pages, what is being loaded, and who these third parties are. We can then access the specific security and privacy implications of these practices.

This study is structured as follows: In Section 2 we describe our study methodology, in Section 3 we present the study results, and then evaluate and discuss the results in Section 4. Finally we present our conclusions in Section 5.

2 Methodology

The online banking portal for each bank was loaded, and the requests to third-parties were recorded for the login page, the online banking site after login, and the logout page. The occurrence of tracking in each of the tested locations has different implications for privacy and security:

- Login page: Tracking occurring here gives a strong indication that the user has an account with this bank. In most cases the online banking portals are separated from the main banking website, so few users are likely to visit this page without an intention to log in to their account. In addition, any third-party which is permitted to load Javascript in the login document will have to ability to read users' login information inputted into this page.
- After login: Tracking here identifies the user as a customer of the bank, and my leak information about banking activities undertaken, such as transfers or loans, if such information can be inferred from the page URL. Again, if third-party Javascript is loaded here, it may read any information displayed in the page, as well as manipulate inputted data.
- After logout: Tracking here will identify the user as a customer of the bank, as users will only land on this page after a valid logged in session. The logout page is unlikely to display private user information, therefore the privacy and security risk from third-party Javascript is reduced.

For the third-parties contacted we noted the following:

- Request type: *Javascript* or *Tracking pixel*.
- Loading context: *Main document* or *iFrame*.
- Tracking utilised: *cookie* and/or *fingerprint*.

As previously mentioned, Javascript requests cause additional security and privacy implications, if this code is also loaded into the main document context. Content loaded into an iFrame context is safer, as this is a sandboxed environment. The tracking method indicates how persistent the tracking ID will be.

The banks tested were:

- ComDirect — `https://kunde.comdirect.de/lp/wt/login`
- Commerzbank — `https://kunden.commerzbank.de/lp/login`
- Consorsbank — `https://www.consorsbank.de/home`
- DAB-Bank — `https://www.dab-bank.de`
- Deutsche Bank — `https://meine.deutsche-bank.de/trxm/db/`

- DKB — `https://www.dkb.de/banking`
- HypoVereinsBank — `https://my.hypovereinsbank.de/login`
- ING DiBa — `https://banking.ing-diba.de/app/login`
- Number26 — `https://my.number26.de`
- PostBank — `https://banking.postbank.de/rai/login`
- Stadtsparkasse Muenchen — `https://homebanking.sskm.de/portal/portal/Starten`
- Volksbank Mittelhessen — `https://www.vb-mittelhessen.de`

The websites were visited on the 7th and 8th July 2016. Logins for the banks tested were provided by volunteers from Cliqz GmbH.

3 Results

We loaded online banking portals for several German banks and gathered data as outlined in the previous section. For each location results are shown in Tables 1, 2 and 3 respectively.

Table 1 shows that most banks have no third-parties on their login pages. Of the those that do:

- Deutsche Bank and DKB show a security seal from Verisign. This seal is created by loading a third-party Javascript into the page. This Script is served with a cookie, and is not cached, so that Verisign will be notified every time a user accesses these pages, and will be able to attribute each access to a single user.
- ComDirect and DKB include a tracking pixel in the login page, from advertising providers Adform and Webtrekk respectively. These use cookies and browser fingerprinting techniques to tracker users accessing this page.
- Consorsbank includes a support chat widget in an iFrame. The use of the iFrame prevents this third party accessing private information in the page, however the use of the cookie would allow them to track users who use this service on other sites.
- Number26 loads several third-party Javascripts into the page, from Facebook, Google and TrackJS. These scripts then send tracking data back to their respective owners.

Table 2 shows again that most banks do not have third-parties after logging into online banking. On those that do:

- Consorsbank has a support chat widget as in the login page.

Bank	Third party	Type	Context	Tracking
Commerzbank	none			
HypoVereinsBank	none			
PostBank	none			
Stadtsparkasse	none			
ING DiBa	none			
DAB-Bank	none			
Volksbank	none			
Deutsche Bank	`seal.verisign.com`	JS	Main	C
ComDirect	`track.adform.net`	Pixel	Main	C
Consorsbank	`eu.ntrsupport.com`	JS	iFrame	C
DKB	`seal.verisign.com`	JS	Main	C
	`seal.websecurity.norton.com`	Pixel	Main	—
	`webtrekk.net`	Pixel	Main	C + FP
Number26	`connect.facebook.net`	JS	Main	—
	`www.google-analytics.com`	Pixel	Main	FP
	`cc-collector.tech26.de`	Pixel	Main	FP
	`cloudfront.net`	JS	Main	—
	`usage.trackjs.com`	Pixel	Main	—
	`doubleclick.net`	Pixel	Main	C + FP
	`google.com`	Pixel	Main	C + FP

Table 1: Third parties on login pages. C denotes cookie and FP denotes Fingerprint.

Bank	Third party	Type	Context	Tracking
Commerzbank	none			
HypoVereinsBank	none			
PostBank	none			
Stadtsparkasse	none			
ING DiBa	none			
DAB-Bank	none			
Volksbank	none			
Deutsche Bank	none			
ComDirect	none			
Consorsbank	`eu.ntrsupport.com`	JS	iFrame	C
DKB	`seal.verisign.com`	JS	Main	C
	`seal.websecurity.norton.com`	Pixel	Main	—
Number26	`connect.facebook.com`	JS	Main	—
	`www.google-analytics.com`	Pixel	Main	FP
	`cc-collector.tech26.de`	Pixel	Main	FP
	`cloudfront.net`	JS	Main	—
	`usage.trackjs.com`	Pixel	Main	—
	`doubleclick.net`	Pixel	Main	C
	`www.google.com`	Pixel	Main	C
	`www.facebook.com`	Pixel	Main	C
	`livechatinc.com`	JS	Main	C + FP

Table 2: Third parties after login. C denotes cookie and FP denotes Fingerprint.

- DKB continues to show the Verisign seal after logging in, allowing Verisign to see what pages the user accesses within online banking.
- Number26 has the same third parties as on the login page in addition to a support chat widget which is loaded directly in the main document. The request to load this widget includes the user's email address and name.

Table 3 shows that several sites are sending tracking data to third parties after their customers log out of online banking:

- Commerzbank, DAB-Bank, ComDirect and Consorsbank all have a tracking pixel from advertising and analytics companies such as Adform, Adition and Omniture.
- DKB includes multiple tracking pixels in the logout page, from Google, Advertising.com, Adition, MathTag, Eyeota, Turn, Semasio, Webtrekk and Netzeffekt.
- Number26 has the same third parties as on the login page and when logged in.

4 Evaluation & Discussion

The results of this survey show that, of the 12 online banking portals tested, only 5 leaked no data to third parties during a typical online banking session (HypoVereinsBank, PostBank, Stadtsparkasse, ING DiBa and Volksbank). When logged in, only 3 sites have third-party requests, 1 of which does so in a safe manner. After logout we see the highest incidence of tracking, with half of the sites sending data to large tracking and analytics companies.

We can infer, from the usual use cases of the third-party companies used, the reasons for their inclusion on the banking sites presented here. There are four prime use-cases we see from this study:

- Site analytics – Software-as-a-Service providers who provide analytics about site usage and performance (e.g. Google Analytics and TrackJS).
- Marketing and Business Intelligence – Advertising companies who help clients track conversions from marketing. Such services might track the bank's users in order to prevent the bank from advertising to existing customers, or to see how many new customers a particular advertising campaign generates. Examples include DoubleClick, Adition, AdForm and Facebook.
- Trust – Companies such as Verisign provide seals which reassure users of the bank's security.
- Support tools – Third party chat support systems allow banks to outsource online support (e.g. LiveChat and NTR).

Bank	Third party	Type	Context	Tracking
Commerzbank	track.adform.net	Pixel	Main	C
HypoVereinsBank	none			
PostBank	none			
Stadtsparkasse	none			
ING DiBa	adition.com	Pixel	Main	C
DAB-Bank	none			
Volksbank	none			
Deutsche Bank	none			
ComDirect	track.adform.net	Pixel	Main	C
Consorsbank	omtrdc.net	JS	Main	FP
DKB	seal.verisign.com	JS	Main	C
	seal.websecurity.norton.com	Pixel	Main	—
	uip.semasio.net	Pixel	Main	C
	1001.netrk.net	Pixel	Main	C
	www.google-analytics.com	Pixel	Main	FP
	doubleclick.net	Pixel	Main	C
	webtrekk.net	Pixel	Main	C + FP
	www.google.com	Pixel	Main	C + FP
	advertising.com	Pixel	Main	C + FP
	mathtag.com	Pixel	Main	C
	d.turn.com	Pixel	Main	C
	eyeota.net	Pixel	Main	C
	adition.com	Pixel	Main	C
Number26	connect.facebook.com	JS	Main	—
	www.google-analytics.com	Pixel	Main	FP
	cc-collector.tech26.de	Pixel	Main	FP
	cloudfront.net	JS	Main	—
	usage.trackjs.com	Pixel	Main	—
	doubleclick.net	Pixel	Main	C
	www.google.com	Pixel	Main	C
	www.facebook.com	Pixel	Main	C
	livechatinc.com	JS	Main	C + FP

Table 3: Third parties on logout page. C denotes cookie and FP denotes Fingerprint.

The use of these services directly benefits the banks, by helping them to optimise business processes, reduce costs, and possibly provide better software tools than what could be produced in-house. However, there are also some risks: security and user privacy.

4.1 Security Implications

Banks have a high security requirement, being prime targets for fraud and hacking. They will likely have stringent internal requirements on IT systems in order to maintain robust security. Introducing third parties into secure parts of their websites risks increasing their attack surface area. For example, and Javascript loaded into the main document is a potential attack vector, as if compromised, it may take complete control of the page and user inputted data. Third parties identified in this study, who have Javascript loaded into bank pages may not have the same security standards as a bank, and thus could be a weak link which gives an attacker access to thousands of bank accounts.

4.2 Privacy Implications

Whenever a third party is contacted in the main page context, they receive information about the page being loaded, via the `Referer` HTTP header, and the IP address of the machine making this request. Coupled with a cookie and/or some kind of browser fingerprint technique, the third party can distinguish unique users accessing this web page. If the third party is used by other sites across the web, they can collect a profile of sites used by particular users. This is a standard practice on the Internet, primarily to target advertising and recommendations based on user interests.

However, which bank one uses is likely for many users to be more sensitive information than, for example, which news articles they read. Furthermore, if tracking occurs within the logged in session, information could be inferred about the user's financial status. Note that we do not believe that data is being used for such purposes, however the technical means used provides the capability for these third-party companies to do this.

We can evaluate the privacy risk from the third parties used in this survey, by measuring the reach of these companies across the web. The greater the reach, the more comprehensive the theoretical user profile. Using data from our anti-tracking software, we can measure this reach, as seen by our users over a two week period, and presented in Table 4.

It should be noted that a reach of 1% is very high – for an average user, one in every hundred pages will receive data. That over half of the third parties has a reach over 1% shows that these companies have the ability to generate significant user profiles, and in most cases over tens or hundreds of thousands of different sites. As we have shown, this profile could include user's bank.

The tracking from these third parties can be mitigated, however, by the use of anti-tracking tools such as Cliqz Anti-Tracking [8]. This will remove the

Third party	Reach	# of sites
google-analytics.com	44.29%	790,000
google.com	36.89%	550,000
www.google.com	29.76%	420,000
doubleclick.net	30.91%	400,000
www.facebook.com	21.11%	310,000
adition.com	7.62&	30,000
mathtag.com	5.43%	42,000
turn.com	3.64%	30,000
track.adform.net	3.47%	45,000
uip.semasio.net	1.90%	12,000
advertising.com	1.43%	25,000
omtrdc.net	1.42%	7,200
webtrekk.net	0.96%	3,500
eyeota.net	0.40%	4,800
seal.websecurity.norton.com	0.19%	1,700
seal.versign.com	0.14%	1,300
livechatinc.com	0.06%	2,200
usage.trackJS.com	0.05%	740
d2zah9y47r7bi2.cloudfront.net	0.03%	510
netrk.net	0.04%	890
eu.ntrsupport.com	0.04%	83
d1fc8wv8zag5ca.cloudfront.net	0.01%	270
tech26.de	<0.01%	5

Table 4: Reach of third parties in terms of percentage of page loads seen (to 2 decimal places) and the number of domains where the third party has been seen (to 2 significant figures)

cookies from the third-party requests, and remove any fingerprint data sent. This effectively prevents the possibility of a user profile.

5 Conclusion

This survey shows the extent of tracking on the online banking portals of German banks. We find that over half of the surveyed banks include tracking at some stage of the online banking process. We discussed the security and privacy implications of this tracking, and provided further evidence of the reach of the trackers being used.

The reasons for the use of these third-party services we cannot know for sure. As we have discussed, these services offer material value to the site owners. Privacy and security side effects may not be known, or have been examined and deemed acceptable. These side effects could change at anytime however, third parties are, by nature, outside of the control of the first party. For example, the sale of a third-party company could trigger the first party's customer data being up for sale [7].

In response to these issues, privacy protecting software is increasingly being adopted to give web users control over what data is sent to third parties on web sites. To name a few, Ghostery [4], Disconnect [1] and Firefox tracking protection [6] use curated block lists to prevent requests being made to known tracking services, and Privacy Badger [5] applies a heuristic approach to blocking of third parties. The Cliqz browser and Cliqz Firefox browser extension use a data-driven approach to preventing tracking, using the crowd to determine which data is safe and which is unsafe [8]. Of the pages tested in this study, Cliqz Anti-Tracking would remove all cookies, and any fingerprinting attempts deemed to be tracking the user.

References

[1] Disconnect. Disconnect. `https://disconnect.me/`.

[2] P. Eckersley. How unique is your web browser? In *Proceedings of the 10th International Conference on Privacy Enhancing Technologies*. Springer-Verlag, 2010.

[3] S. Englehardt and A. Narayanan. Online tracking: A 1-million-site measurement and analysis. [Technical Report], May 2016.

[4] Ghostery. Ghostery. `https://ghostery.com/`.

[5] H. P. Jason Bau, Jonathan Mayer and J. C. Mitchell. A promising direction for web tracking countermeasures. In *Proceedings of Web 2.0 Security and Privacy (W2SP)*. IEEE Computer Society, 2013.

[6] G. Kontaxis and M. Chew. Tracking protection in firefox for privacy and performance. In *Proceedings of Web 2.0 Security and Privacy (W2SP)*. IEEE Computer Society, 2015.

[7] A. Peterson. Bankrupt radioshack wants to sell off user data. but the bigger risk is if a facebook or google goes bust. Washington Post, March 26th 2015.

[8] Z. Yu, S. Macbeth, K. Modi, and J. M. Pujol. Tracking the trackers. In *Proceedings of the 25th International Conference on World Wide Web*, pages 121–132. International World Wide Web Conferences Steering Committee, 2016.