

# SCH<sub>ELL</sub>MANCON

 schellman

  
jscrambler



# Seal the Browser Leak: Addressing Compliance and Data Protection Challenges

---

**John Elliott**

SECURITY ADVISOR AT JSCRAMBLER



jscrambler

**SHELLMANCON**



**Did you notice that we  
broke the internet?**

We went from this



SHELLMANCON

To this



SHELLMANCON

# Agenda



- › What's the big problem?
- › The three threats
- › What is the regulatory view?
- › What should we do?



# What's the problem?

SHELLMANCON





# Every bit of JavaScript has access to any page element.

(I am excluding cross-domain or sandboxed iframes from this discussion)





Which means it can...

**read**

**alter**

**steal**

...anything on the page



**Do you trust every bit  
of JavaScript?**



Because it has access to...

**Any data  
entered by  
the user**

**Anything  
displayed**

**Events**

**URL &  
some  
cookies**



Because it can...

**Send data  
anywhere**

**Hijack  
events**

**Add extra  
code**

**Change  
behavior**



Frameworks

Libraries

Personalization

A/B Testing

Tag Managers

Chat

User behaviour

Cookie / Privacy

Marketing

Social Media

Analytics

Advertising

Shipping

Tax

Location

Payments



**How big  
is this?**



**100**  
Scripts

**52%**  
First party

**48%**  
Third party

*Source: Jscrambler research*

**SHELLMANCON**





**100**  
Scripts

**13**  
Domains  
(mean)

**35**  
Domains  
(max)

*Source: Jscrambler research*

**SHELLMANCON**



# The Threats

That cause data to leak from browser

SHELLMAN&KON



## The Threats

**Covert**

**Configuration**

**Criminal**



# 1. “Covert”



# Health data exposed by Meta “pixel”

<https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

*Health advertising on Facebook: Privacy and policy considerations.* Patterns. Vol 3, Issue 9. September 2022. Downing A, Perakslis E

<https://www.sciencedirect.com/science/article/pii/S2666389922001726>

# Third-party JavaScript on hospital websites



Company	Number (n=3,747)	Percentage
Alphabet	3,691	98.5%
Meta	2,083	55.6%
Adobe Systems	1,177	31.4%
AT&T	992	24.6%
The Trade Desk	813	21.7%
Oracle	802	21.4%
Verizon	791	21.1%
Rubicon Project	712	19%
Amazon	689	18.4%
Microsoft	671	17.9%

*Widespread Third-Party Tracking On Hospital Websites Poses Privacy Risks For Patients And Legal Liability For Hospitals.*  
Health Affairs. Vol 42, No 4. April 2023. Friedman et al.

<https://www.healthaffairs.org/doi/epdf/10.1377/hlthaff.2022.01205>

**SHELLMANCON**



# 2. Configuration





# Tax filling data

<https://themarkup.org/pixel-hunt/2022/11/22/tax-filing-websites-have-been-sending-users-financial-information-to-facebook>

# Abortion advice

<https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients>



# 3. Criminal





## The attack surface

**First party**

**Third party**

**Tag manager**



## The attack surface

**First party**

**Third party**

**Tag manager**



## The attack surface

**First party**

**Third party**

**Tag manager**





## The attack surface

**First party**

**Third party**

**Tag manager**





## Tag manager

<https://geminiadvisory.io/threat-actors-continue-to-abuse-google-tag-manager-for-payment-card-e-skimming/>

## Expired domains

<https://blog.jscrambler.com/defcon-skimming-a-new-batch-of-web-skimming-attacks/>

## Web Sockets

<https://www.akamai.com/blog/security/magecart-attack-disguised-as-google-tag-manager>



**Hostile threat actors will use JavaScript skimming techniques to exfiltrate more than just cardholder data.**



# Regulatory Views?

SHELLMANCON



## Four “regulators” actions

**Payment Card  
Industry  
(PCI DSS)**

**UK Information  
Commissioner  
(GDPR)**

**Federal Trade  
Commission**

**Health and Human  
Services (HIPAA)**



## Four “regulators” actions

**Payment Card  
Industry  
(PCI DSS)**

**UK Information  
Commissioner  
(GDPR)**

**Federal Trade  
Commission**

**Health and Human  
Services (HIPAA)**



## PCI DSS 4.x | Requirement 6.3.4 (2025)

**Inventory**

**Authorized**

**Necessary**

**Integrity  
validated**



## PCI DSS 4.x | Requirement 11.6.1 (2025)

Changes in  
headers

Changes in  
content

< 7 days

Alert





## Four “regulators” actions

**Payment Card  
Industry  
(PCI DSS)**

**UK Information  
Commissioner  
(GDPR)**

**Federal Trade  
Commission**

**Health and Human  
Services (HIPAA)**



## UK ICO | GDPR | Ticketmaster\*

“Ticketmaster ought reasonably to have been aware prior to the time of the Incident of the risk of implementing third party JavaScripts into a web site that processes personal data such as payment card data.”

<https://ico.org.uk/media/action-weve-taken/2618609/ticketmaster-uk-limited-mpn.pdf>

\* Subject to appeal



## UK ICO | GDPR | Ticketmaster\*

“Because the payment page processed personal data, Ticketmaster should have risk-assessed the implementation of third-party scripts into this page.”

<https://ico.org.uk/media/action-weve-taken/2618609/ticketmaster-uk-limited-mpn.pdf>

\* Subject to appeal



## Four “regulators” actions

**Payment Card  
Industry  
(PCI DSS)**

**UK Information  
Commissioner  
(GDPR)**

**Federal Trade  
Commission**

**Health and Human  
Services (HIPAA)**



## FTC | Health Breach Notification | GoodRX

“GoodRx violated the FTC Act by sharing sensitive personal health information for years with advertising companies and platforms—contrary to its privacy promises—and failed to report these unauthorized disclosures as required by the Health Breach Notification Rule..”

<https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc>



## Attacks on Tax Privacy:

How the Tax Prep Industry Enabled Meta to Harvest Millions of Taxpayers' Sensitive Data



Prepared by the Offices of Senators Elizabeth Warren, Ron Wyden, Richard Blumenthal, Tammy Duckworth, Bernie Sanders, and Sheldon Whitehouse, and Representative Katie Porter

July 2023

## FTC | ???? | Tax Preparation Companies

“For this reason, we urge the Department of Justice (DOJ), the IRS the U.S. Treasury Inspector General for Tax Administration (TIGTA), and the Federal Trade Commission (FTC) to immediately open an investigation into this incident.”

[https://www.warren.senate.gov/imo/media/doc/Attacks%20on%20Tax%20Privacy\\_Final.pdf](https://www.warren.senate.gov/imo/media/doc/Attacks%20on%20Tax%20Privacy_Final.pdf)

**SHELLMAN** AND ASSOCIATES



## Four “regulators” actions

**Payment Card  
Industry  
(PCI DSS)**

**UK Information  
Commissioner  
(GDPR)**

**Federal Trade  
Commission**

**Health and Human  
Services (HIPAA)**





## Office of Civil Rights (OCR) | Health & Human Services (HHS) | HIPAA | Hospitals

“Regulated entities are required to comply with the HIPAA Rules when using tracking technologies.”

<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>



## Office of Civil Rights (OCR) | Health & Human Services (HHS) | HIPAA | Hospitals

- Permitted by the Privacy Rule
- Have a Business Associate agreement in place
- Risk assessment & comply with Security Rule
- Breach notification otherwise

<https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>



## Office of Civil Rights (OCR) | Health & Human Services (HHS) | HIPAA | Hospitals

### **Hospitals:**

It's OK because Meta deletes all health information it receives

### **OCR:**

“it is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives”



# Office of Civil Rights (OCR) | Health & Human Services (HHS) | HIPAA | Hospitals

## Hospitals:

It's OK because Meta deletes all health information it receives

## OCR:





**Managing the risk associated with JavaScript that executes in your customers' browsers will become an explicit or implicit (*reasonable, appropriate*) regulatory requirement.**

# Differing regulatory approaches



Manage this

Do reasonable  
(appropriate)  
things

Objective / Outcome

Make this  
happen

Prescriptive

Do *all these  
things*



**100**  
Scripts

**52%**  
First party

**48%**  
Third party

*Source: Jscrambler research*

**SHELLMANCON**





**Managing JavaScript is going to be painful for many organizations.**

## Where we might start



**Regulators'  
view of what  
is reasonable**

**The  
practicality of  
managing  
JavaScript**



**Initially there will be a disconnect between what a regulator thinks is reasonable and what is practical.**

**Documented risk assessments will be key.**

## PCI SSC: Example of “Regulatory” “Dithering”



- PCI DSS v4 (March 2022)  
Manage JavaScript in the payment page from April 2025
- Manage JavaScript in the parent page SAQ A (April 2022)
- Manage JavaScript in the parent page (June 2024)
- ~~Manage JavaScript in the parent page SAQ A (January 2025)~~
- We didn't really mean that (February 2025)





# What Can You Do Today?

Prepare For Risk Management & Regulation

SHELLMANCON

Next week



Make an inventory of all the  
JavaScript on your website

**All pages /  
sections**

**First party**

**Third party**



Next week



Discover who owns them

Who added?  
Why?

Is there a  
process?

Tag manager?

In two months



## Risks assessment

**“Covert”**

**Configuration  
errors**

**Criminal**

In three months



What will you need to do if (when)  
you need to comply with regulation?

**What's the best  
business  
process?**

**Pre- or post-  
approval?**

**Can you zone-  
segment the  
site?**

After that



Evaluate technical solutions that fit  
with your business processes

**Business  
change activity**

**Always PoC**

**Fits you**

**SHELLMANCON**

## Predictions summary



- 1 Hostile threat actors will use JavaScript skimming techniques to exfiltrate more than just cardholder data.
- 2 Managing the risk associated with JavaScript that executes in your customers' browsers will become a regulatory requirement.
- 3 Managing JavaScript will be painful for many organizations.
- 4 There will be a disconnect between regulatory opinion and what is practical. Documented risk assessments will be key.



## Thank You

[www.schellman.com](http://www.schellman.com)

[info@schellman.com](mailto:info@schellman.com)

1.866.254.0000

Int'l +1.813.288.8833

Follow @Schellman on Social Media:



[john.elliott@jscrambler.com](mailto:john.elliott@jscrambler.com)

**SHELLMANCON**