

TLP:WHITE

## INDUSTRY REPORT

# RH-ISAC Benchmark Report

Q3 2019

EXPOSING DIGITAL SHADOW IT:  
Identifying third-party code and its impact on and  
risk to retail and hospitality eCommerce  
transactions.



THE MEDIA TRUST  
We know digital security.

RETAIL & HOSPITALITY  
ISAC

# TABLE OF CONTENTS

- Introduction..... 2
- Third-Party Code Rewards and Risks..... 2
- Key Areas of Interest ..... 4
- Benchmark Best-In-Class ..... 5
  - Path to Best-In-Class ..... 5
  - Perspectives and lessons learning ..... 7
  - Timeline For Improvements ..... 8
- About This Benchmark ..... 9
  - Scanning Methodology ..... 9
  - Comprehensive Client-Side Scanning..... 9
  - Research Partners ..... 10

# Introduction

Breaches and security failures via websites of leading household names continue to dominate the headlines. A common denominator is the presence and compromise of a third-party vendor operating in the digital environment.

The Retail & Hospitality ISAC partnered with The Media Trust to raise awareness of this concern among RH-ISAC members and the broader retail community. A key function of our partnership involves customer transactions and scans of websites in our industry sector, and the identification of third-party visibility into and impacts on those transactions. This report highlights the 2019-Q3 findings of 23 eCommerce web sites across retail, restaurant/QSR, and hotel/gaming/casino enterprises within our sectors.

This benchmark will serve as a tool for enterprises to measure their ability to manage third-party risk in their digital environments. If not properly managed, third-party vendors can affect transaction security, violate data protection regulations, and tarnish the customer experience, which all affect long-term revenue.

## Third-Party Code Rewards and Risks

Most of the technology that powers the digital experiences your customers crave wasn't developed by your in-house teams. Consider the CRM systems, shopping carts, online chat tools, video delivery platforms, social sharing apps, and more that make up just a few clicks on today's digital properties. Market leaders in the retail, restaurant, and hospitality sectors can't operate without this useful functionality, but few understand the scope of what executes when a customer accesses their website. For them this is "Digital Shadow IT".

Beyond GitHub and libraries, enterprises increasingly rely on third-party code to provide the infrastructure and functionality to deliver the features today's consumers expect: dynamic content, personalization, and seamless engagement. This Digital Shadow IT operates outside the scope of the enterprise technology operations, which means this type of third-party code is not monitored and, therefore, there is no warning when it is compromised.

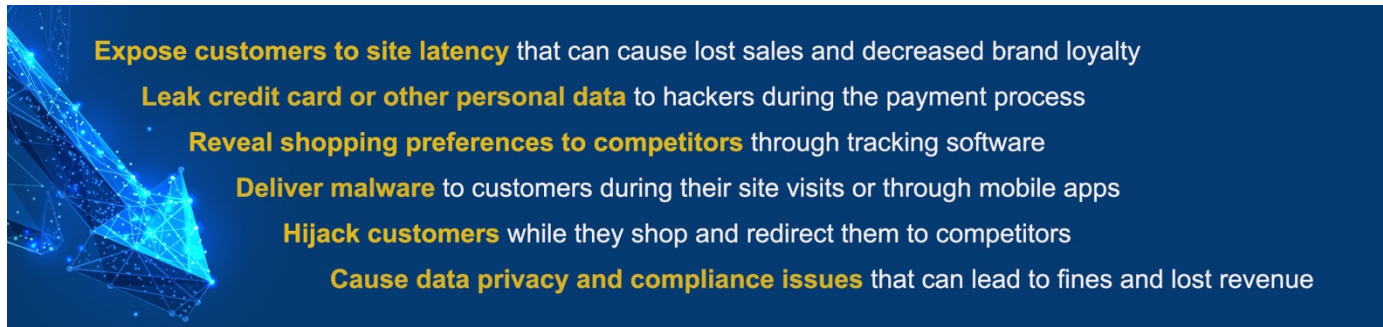
The use of iframes does not protect a website from compromise. Frequently used on payment pages, iframes allow the insertion of another HTML document (i.e., payment processing platform) into a page and isolate its code from other page elements. While iframes narrow the attack surface, they don't eliminate it.

During the page build process, iframes need to be created before execution of an offending script. If this doesn't occur, the page is vulnerable to compromise via switching out the iframe code or removing/hiding it from user view. These techniques enable payment processor spoofing.

**Iframe security failure:** Early Magecart incidents injected JavaScript in the header of payment pages. The code created a transparent overlay on the payment form to collect the payment details entered by the user, drop a cookie, and flash an error upon submission. To cover the malicious activity, the code asked the user to re-key the information, and the cookie identified the user and directed to the valid payment processor.

In scans of over one billion web pages in the last twelve months, The Media Trust confirmed that consumer-facing websites incorporate between 65% to 95% third-party code. This code executes dynamically on consumer devices and varies based on geography, browser type, user profile, and browser history. Because of this, scanning techniques developed by internal teams miss the majority of today's attack vectors.



When third-party code isn't managed properly, it can:



- Expose customers to site latency** that can cause lost sales and decreased brand loyalty
- Leak credit card or other personal data** to hackers during the payment process
- Reveal shopping preferences to competitors** through tracking software
- Deliver malware** to customers during their site visits or through mobile apps
- Hijack customers** while they shop and redirect them to competitors
- Cause data privacy and compliance issues** that can lead to fines and lost revenue

# Key Areas of Interest

Third-party code executing in eCommerce sites can affect a site’s overall operation, from the benign unnecessary calls and changing digital risk footprint to the more serious unauthorized data to collection and overt compromise.

 <p>Overall Latency</p>	<p>Customers are becoming much less forgiving about site speed and expect great performance regardless of their device or network connection. Any latency greater than 3 seconds increases digital risk including shopping cart abandonment.</p>
 <p>New Domains Per Month</p>	<p>Digital properties change more often than most enterprises realize. New domains can mean more opportunities for bad actors to hijack code or the customer experience.</p>
 <p>Excessive Use of Cookies with Long Lifespan</p>	<p>The prying eyes of long-life cookies can capture your site visitor browsing history, then use it for remarketing or customer journey hijacking.</p>
 <p>Domains on payment pages</p>	<p>Security practices dictate that only payment processing domains should be allowed on pages that collect credit card information, i.e., payment page.</p>
 <p>JavaScript Download Size</p>	<p>Third-party JavaScript can make unauthorized calls, be compromised without your knowledge, and slow down page execution. The Media Trust detected 1.62MB of JavaScript, on average, brought by third parties that are not under internal control.</p>

# Benchmark Best-In-Class

Across the benchmark, the companies with the least digital risk exposure from third-party code exhibited the following characteristics (*how does your organization measure up?*):



**New Domains Per Month:** Less than 10%



**Average latency:**  
Less than 2 seconds



**Total JavaScript download size:**  
Less than 1MB



**Cookie lifespan < 12months:**  
Less than 5%



**Domains on payment pages:**  
1

## PATH TO BEST-IN-CLASS

Leading companies don't ignore the risks associated with third-party code, yet sometimes find themselves overwhelmed by the scope of the problem. If a scan reveals serious issues in an organization's digital ecosystem, where should the remediation begin? No single department can handle this effort alone as it touches technology, legal, product, sales, and marketing teams.

Leaders should create a cross-disciplinary team to address the digital challenge. Using the scans and insights from The Media Trust, the team can better understand the scope of the problem, set priorities, develop strategies, and review progress.

Initial steps for addressing digital risk include:

- Identifying and blocking domains that pose immediate security risks based on client-side scans;
- Reviewing payment processing and user profile pages for the third-party domains, code, and tracking systems that could pose a security threat;
- Working proactively with digital vendors through The Media Trust network to communicate policies and procedures and verify compliance; and
- Prioritizing other changes to the digital environment based on the organization's objectives and resources.



## PERSPECTIVES AND LESSONS LEARNING

The initial benchmarking revealed:

- Increasing reliance on third-party vendors;
- Challenges that tend to increase the risk of data leakage;
- Unmanaged code that impacts the customer experience; and
- Evidence that attack vectors can increasingly permeate the customer booking journey.




The above leads to the perspective that eCommerce retailers must place greater emphasis on:

				
<b>Vendor Visibility</b>	<b>Payment Pages</b>	<b>Third-party Code</b>	<b>Cookie Drops</b>	<b>Vendor Communication</b>
Gain greater visibility into how their digital ecosystem changes over time so that they can better assess risks.	Deploy better security on payment pages to prevent major security breaches and resulting reputational damage.	Minimize domain calls and third-party code to provide site visitors a more streamlined experience.	Understand the sources and functions of all cookies dropped on visitors that can collect personal data and re-use for competitor re-marketing.	Maintain better communications with digital third-party vendors who provide code to the user experience that is typically <i>not</i> monitored by enterprise IT teams



## TIMELINE FOR IMPROVEMENTS

The Media Trust has helped hundreds of customers reduce digital risk and protect revenue from bad actors. Using the insights provided, executive teams can see a marked improvement in 90 days.

TIMELINE FOR IMPROVEMENTS	
 <b>Month 1</b>	<ul style="list-style-type: none"><li>• Identify the Digital Risk Management Team</li><li>• Review The Media Trust Scans</li><li>• Block Bad Actors</li><li>• Improve Payment Processing Pages</li></ul>
 <b>Month 2</b>	<ul style="list-style-type: none"><li>• Review The Media Trust Scans</li><li>• Understand Digital Environment Changes</li><li>• Identify High-Impact Fixes</li><li>• Digital Vendor Policy Enforcement</li></ul>
 <b>Month 3 and Beyond</b>	<ul style="list-style-type: none"><li>• Review The Media Trust Scans</li><li>• Understand Digital Environment Changes</li><li>• Prioritize Security and Speed Enhancements</li><li>• Continue Policy Enforcement</li></ul>

# About This Benchmark

## SCANNING METHODOLOGY

The Media Trust leverages its proprietary website, mobile app and ad tag SaaS-based service to scan public-facing websites on a continuous, 24/7 basis using a series of user profiles to replicate a true visitor experience. This client-side monitoring identifies all vendors—third, fourth and sometimes fifth parties—executing on the website, assesses for security vulnerabilities, analyzes data collection activities, and detects performance issues.

The information contained in this report was collected during the stated time frame using a generic scanning algorithm and basic desktop-only user profiles. It does not address mobile or gaming devices, targeted user behavior profiles, geographies nor scanning rates specific to an enterprise. In addition, the report does not encompass any advertising or revenue-generating tags on website. A true digital risk management solution is customized to provide continuous insight and control of the third-party vendors executing on the website to easily detect and terminate any malicious, unauthorized, noncompliant or performance-sapping activity.

## COMPREHENSIVE CLIENT-SIDE SCANNING

Comprehensive, client-side scanning is the best method for protecting websites and customers from third-party malware attacks. With a presence in 550 cities across more than 100 countries, The Media Trust scans more than 10 million of the world's most heavily trafficked websites and leads a network of digital vendors who are committed to promoting a healthy online environment for consumers. The Media Trust clients have access to tools that allow them to share policies and procedures with these digital vendors; a critical piece of compliance for data privacy regulations including GDPR and CCPA. Through this network, The Media Trust knows:

- **Third-party domains called from digital properties**, including the total number of domains and the new domains that have been added in the last 30 days;
- **JavaScript executing in the browser or mobile apps**, including average download size and any malware or suspicious code;
- **Tracking cookies**, including the length of time they are set to collect data and the average number delivered through the site;
- **Average download size** of site pages in MBs, which can be used as a measurement for improving the browsing experience;
- **Average latency** in seconds, indicating where third-party code could impact site speed.



## RESEARCH PARTNERS

### ***RH-ISAC***

The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) is the trusted community for sharing sector-specific cyber security information and intelligence. The RH-ISAC connects information security teams at the strategic, operational and tactical levels to work together on issues and challenges, to share practices and insights, and to benchmark among each other – all with the goal of building better security for the retail and hospitality industries through collaboration. RH-ISAC serves all retail and hospitality companies, including retailers, restaurants, hotels, gaming casinos, food retailers, consumer products and other consumer-facing companies. For more information, visit [www.rhisac.org](http://www.rhisac.org).

### ***The Media Trust***

The Media Trust is on a mission to fix the digital ecosystem. Through continuous monitoring of websites and mobile apps, we provide transparency into the complex relationships delivering the consumer experience. More than 600 premium enterprises, media publishers, ad networks/exchanges, and agencies—including 40 of comScore's AdFocus Top 50 websites—rely on The Media Trust to identify and remediate security, data protection and quality risks which can lead to regulatory fines, depressed inventory value, revenue loss and brand damage. For more information, visit [www.mediatrust.com](http://www.mediatrust.com).

