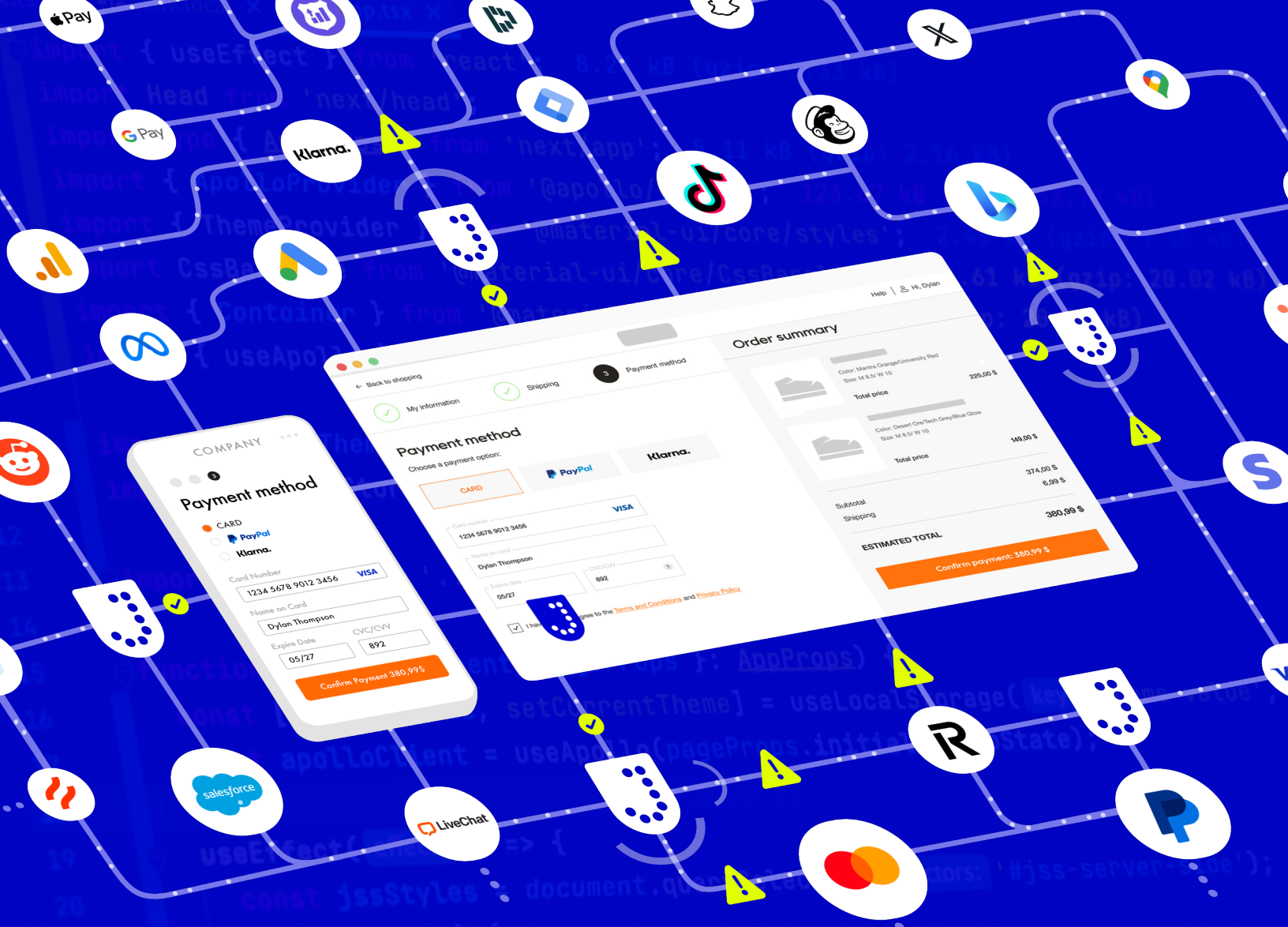


The Perils of Third-Party Tags

Examining the Client-Side Security Risks and Compliance Challenges of JavaScript

jscrambler

jscrambler

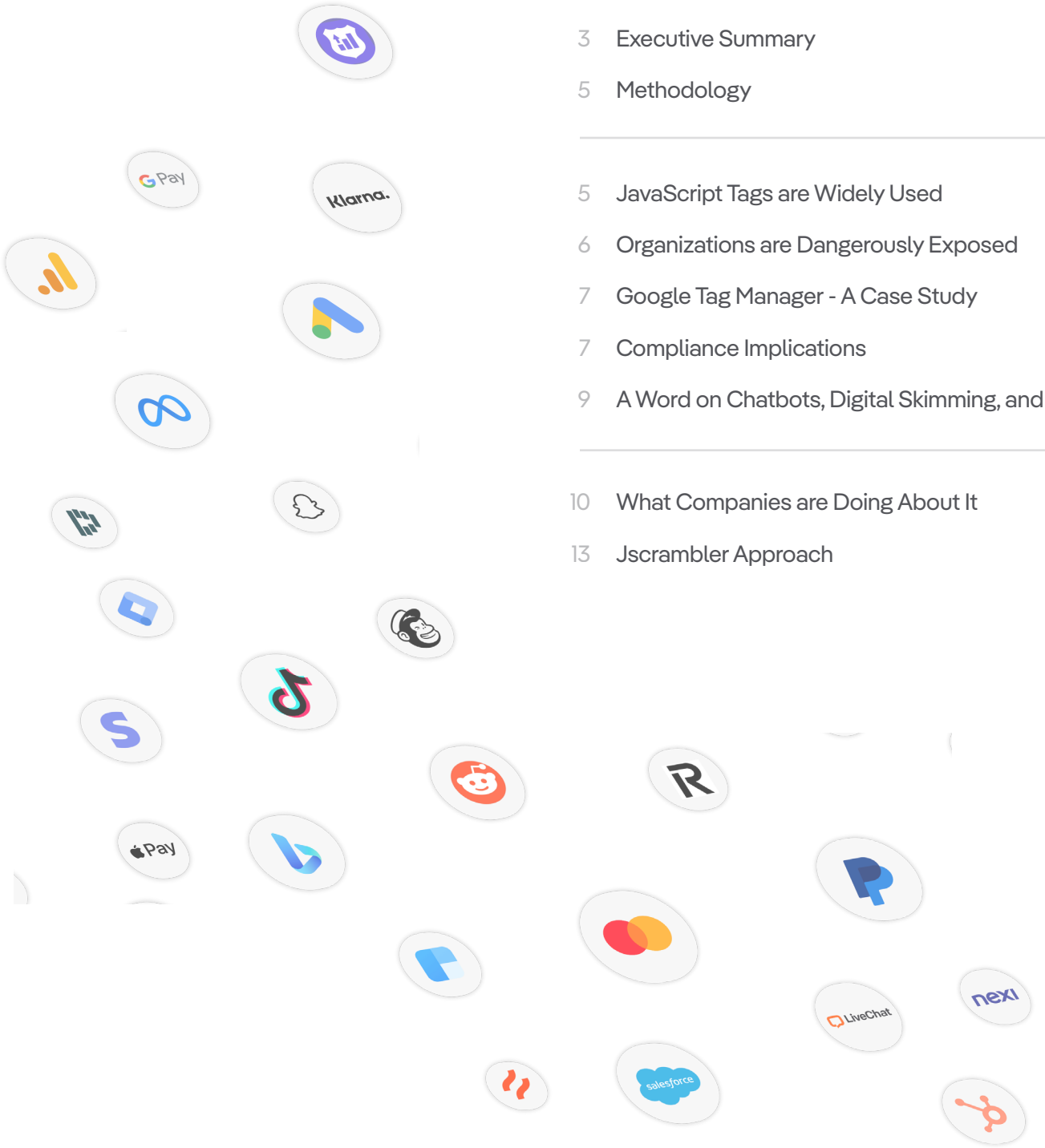


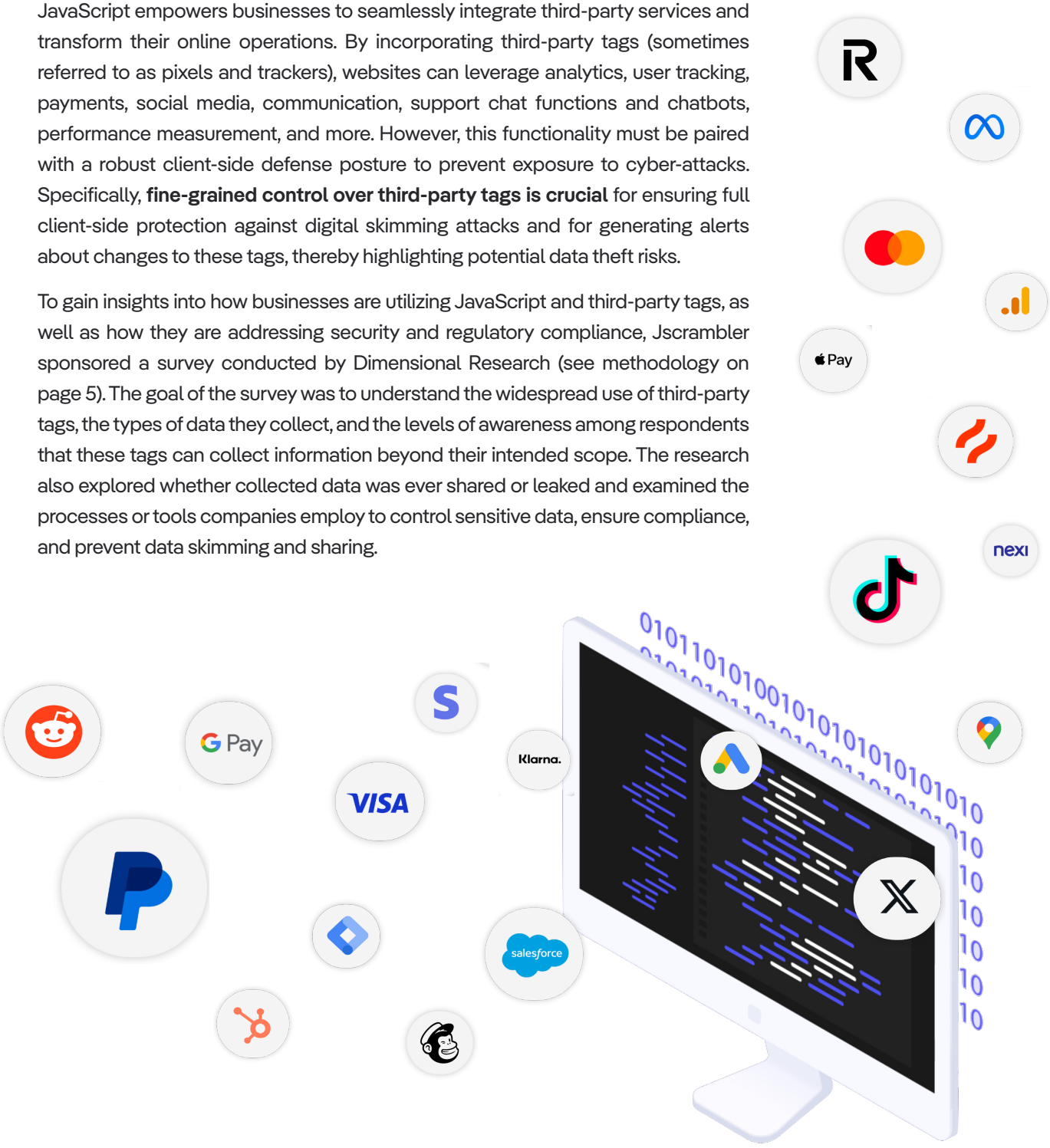
Table of Contents

jscrambler

Executive Summary

JavaScript empowers businesses to seamlessly integrate third-party services and transform their online operations. By incorporating third-party tags (sometimes referred to as pixels and trackers), websites can leverage analytics, user tracking, payments, social media, communication, support chat functions and chatbots, performance measurement, and more. However, this functionality must be paired with a robust client-side defense posture to prevent exposure to cyber-attacks. Specifically, **fine-grained control over third-party tags is crucial** for ensuring full client-side protection against digital skimming attacks and for generating alerts about changes to these tags, thereby highlighting potential data theft risks.

To gain insights into how businesses are utilizing JavaScript and third-party tags, as well as how they are addressing security and regulatory compliance, Jscrambler sponsored a survey conducted by Dimensional Research (see methodology on page 5). The goal of the survey was to understand the widespread use of third-party tags, the types of data they collect, and the levels of awareness among respondents that these tags can collect information beyond their intended scope. The research also explored whether collected data was ever shared or leaked and examined the processes or tools companies employ to control sensitive data, ensure compliance, and prevent data skimming and sharing.



jscrambler

Knowledge Gaps Abound: Surprisingly, only 13% of surveyed participants are extremely confident they know exactly what information third-party tags are collecting. Nearly every respondent (97%) indicated that third-party tags regularly collect sensitive or private information, and 49% admitted that these tags have collected data they were not supposed to.

For instance, over 90% of respondents are familiar with Google Tag Manager, but only 33% recognize that teams using it can autonomously add more third-party tags and code without additional authorization, creating compliance and security risks.

13%
Companies extremely confident they know exactly what information third-party tags are collecting

Protocols in Place: What are companies doing to mitigate security risks and impending compliance requirements? Only 36% have policies and tools in place to prevent data skimming. With 26% of companies aware that sensitive data has been leaked to another organization solution adoption still remains low.

36%
Companies indicated having policies and tools in place to prevent data skimming

A Wake-Up Call: 68% of respondents agree that a client-side protection and compliance solution should be deployed to protect user data from being collected, skimmed, or leaked to third parties. Additionally, 61% stated that such a solution would aid in ensuring PCI DSS compliance.

Furthermore, an overwhelming 97% indicated that a client-side protection and compliance solution would be valuable to their company. This consensus highlights the critical need for enhanced client-side protection measures.

97%
Companies indicated that a client-side protection and compliance solution would be valuable

Methodology

The survey was administered by Dimensional Research electronically. Roles responsible for websites (IT, cyber security, product management, marketing, etc.) at medium-sized and enterprise companies representing all seniority levels were invited to participate in a survey on their company's use of third-party tags.

A total of 327 qualified participants completed the survey. All participants had enterprise responsibilities within IT operations, infrastructure, architecture, cybersecurity, or product management. Participants were from five continents, ensuring the findings comprise a global perspective. Of the respondents, 74% have responsibility for the technical aspects of their organizations' websites.

Findings

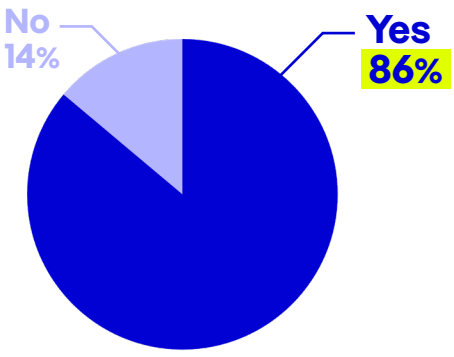
JavaScript Tags Are Widely Used

Respondents know they're benefitting from tag use.

The survey results reveal that 86% of respondents' companies use third-party tags (partners, vendors, etc.) on their websites. Jscrambler analysts report that the average customer acknowledges using over 60 tags, indicating that use is extensive.

According to Radixweb research, 98.7% of websites use JavaScript as a client-side programming language. That's 42.5 million websites worldwide that benefit from the use of tags. On the flip side, that's a lot of security exposure for threat actors to exploit. With stolen data, including payment card information and personal or company information from input fields, the risk is substantial.

Does your company use third-party tags (partners, vendors, etc.) on your website?

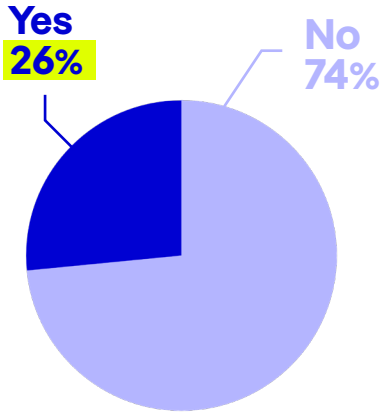


Organizations Are Dangerously Exposed

A substantial gap emerges between the level of knowledge about what tags do and the extent to which they expose sensitive data.

While 97% recognize that tags collect sensitive or private information, only 26% are aware their sensitive data has been leaked to another organization. Third-party tags can contain malicious code, including malware or tracking software, that could compromise a website's security and its users' privacy.

Over the last 12 months was your company aware that sensitive data collected by a third-party tag was leaked to another organization?



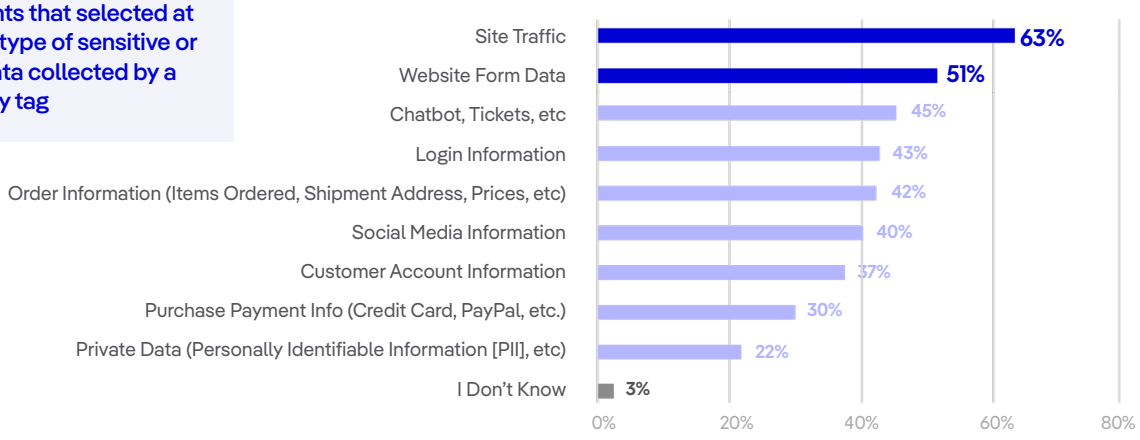
The types of private or sensitive information collected by third-party tags is extensive. As illustrated below, respondents report that data collected includes everything from site traffic data to customer account information, payment information (think credit cards, PayPal, etc.), and PII (Personally Identifiable Information).

This type of data exposure is very lucrative for threat actors. According to Privacy Affairs research, PII can be worth more than $1,000 on the dark web.

What information do the third-party tags on your company's website access?

97%

Participants that selected at least one type of sensitive or private data collected by a third-party tag



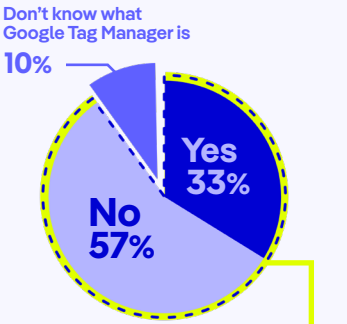
Google Tag Manager
A CASE STUDY

Google Tag Manager (GTM) is an illustrative example of the value of tag use juxtaposed against the lack of users understanding the potential risk.

According to Google, "Tag Manager gives you the ability to add and update your own tags for conversion tracking, site analytics, remarketing, and more. There are nearly endless ways to track activity across your sites and apps, and the intuitive design lets you change tags whenever you want." Widely adopted, fully **90% of respondents are familiar with Google Tag Manager.**

The bad news is that only **33%** realize that it enables teams to autonomously add third-party tags and code without additional authorization. A bit more encouraging, 47% confirm that Google Tag Manager creates privacy and compliance risks.

Did you know that Google Tag Manager enables teams to add third-party tags and code without additional authorization?



90% Companies familiar with Google Tag Manager

33%
Realize Google Tag Manager enables autonomous adding of third-party tags without authorization

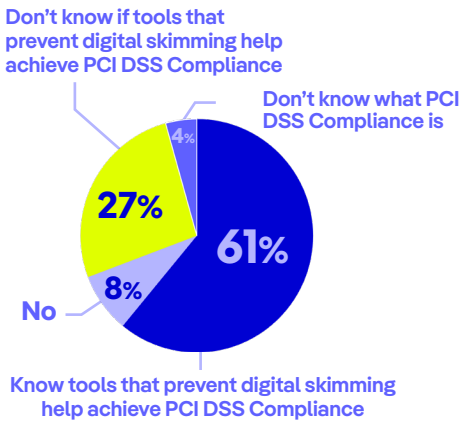
Compliance Implications

Recognition lags with regard to the importance of digital skimming prevention and third-party tag auditing.

Considering that compliance implications for third-party vendor tag use are becoming more pronounced, it is encouraging that **61% state that a tool that prevents digital skimming is key to achieving PCI DSS compliance**. And 57% audit third-party tags to ensure data collection authorization and compliance.

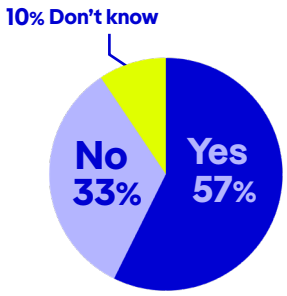
Gaining control over the behavior and data consumption of third-party tags is instrumental in helping organizations meet compliance with various standards, regulations, and laws, including PCI DSS, DORA, GDPR, and HIPAA.

In your experience, will a tool that prevents digital skimming help achieve PCI DSS compliance?



The PCI Security Standards Council (PCI SSC), an international body committed to establishing data security protocols for secure global payments, recently introduced PCI DSS v4, which became mandatory on April 01, 2024. It contains an updated set of guidelines and requirements to ensure that cardholder data is handled, stored and transmitted securely during payment card transactions and includes specific rules for how JavaScript is used on payment pages. Included are requirements 6.4.3 and 11.6.1, which become effective on April 1, 2025.

Does the company regularly audit the third-party tags used on its websites?



PCI DSS v4 Requirement

6.4.3

This requirement aims to reduce vulnerabilities and oversee all JavaScript utilized on payment pages. It requires businesses to follow an approval and justification process for all scripts they integrate into payment pages. The goal is to actively manage all JavaScript elements on these pages and ensure their integrity.

PCI DSS v4 Requirement

11.6.1

The 11.6.1 new requirement focuses on detecting unauthorized modifications to payment pages, which could signal a potential skimming attack. Apart from identifying changes, this requirement stipulates that an alert must be generated whenever any such alterations are detected, although it doesn't mandate that the changes be immediately blocked.

Any organization that wishes to process transactions using payment cards issued by PCI SSC participating card brands (American Express, Discover, JCB, MasterCard, and Visa) will be contractually obliged to comply with PCI DSS.

A Word On Chatbots, Digital Skimming, and Artificial Intelligence (AI)

Digital Skimming

93%
Are knowledgeable about digital skimming, but only 36% have policies and tools to prevent it.

68%
Agree that a client-side protection and compliance solution should protect user data from being skimmed or leaked by third parties.

61%
State a tool that prevents digital skimming is key to achieving PCI DSS compliance.

Chatbots

25%
Cannot ensure sensitive data entered into a chatbot is not shared with other third-parties (only 52% can ensure).

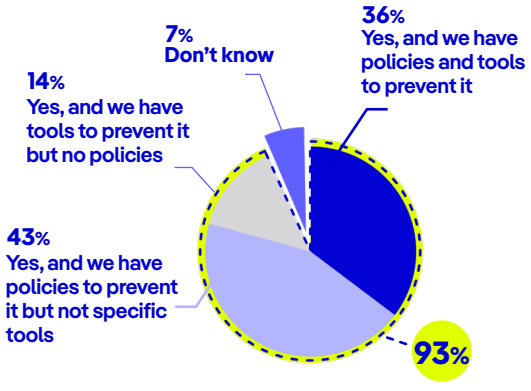
AI

40%
Cannot prevent sensitive data from being entered into a public AI-powered application.

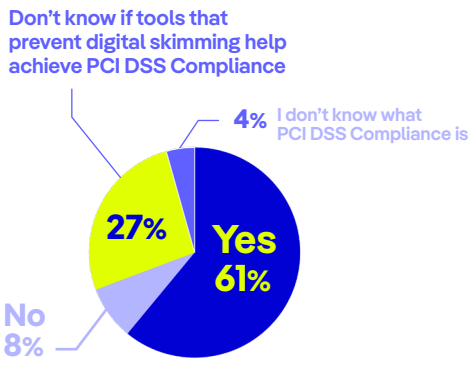
The survey also sought to gain some insight into risks with the increasing use of chatbots and AI, as well as explore the current state of digital skimming risk and prevention.

Digital Skimming

Alarmingly, while 93% of respondents are knowledgeable about digital skimming, only 36% have policies and tools to prevent it. 68% agree that a client-side protection and compliance solution should be deployed to protect user data from being skimmed or leaked by third parties. In addition, **61% agree that a tool that prevents digital skimming is key to achieving PCI DSS compliance**. As March 31, 2025 approaches, PCI DSS compliance will become a more pronounced driver for higher awareness and digital skimming prevention solution adoption.



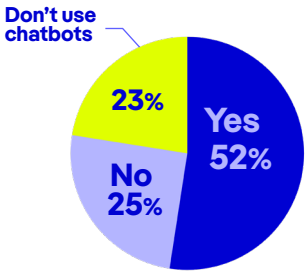
Have you heard about digital skimming?



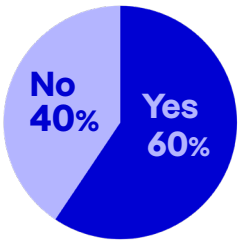
In your experience, will a tool that prevent digital skimming help achieve PCI DSS Compliance?

Chatbots

According to a Techreport Guide, the global chatbot market will exceed $10 billion by 2025 as adoption rates multiply across sectors. Recent surveys reveal that 67% of consumers already utilize chatbots for quick, seamless interactions. With this growth and current use, only 52% of respondents' companies can ensure that sensitive data put into their company's chatbot is not shared with a third party. Once again, policies and tool use appear to be lacking among survey respondents' companies.



Is your company able to ensure sensitive data entered into your company's chatbot is not shared with other third-parties?



Is your company confident they can control sensitive data from being entered into a public AI-powered application?

AI

Continuing with the implications of burgeoning AI adoption, 40% of respondents indicated their companies can't prevent private data from being entered into a public AI-powered application. A key theme at the 2024 Black Hat event, the benefits and risks of AI use, has long since reached mainstream media. An approach using policies and tools to prevent private data from becoming public through AI tools has increasing importance as AI companies compete through the pervasive collection of data.

What Companies Are Doing About It

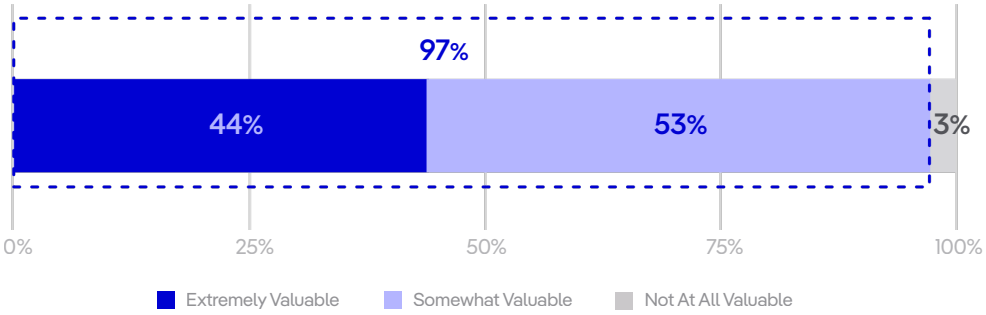
68% Agree that a solution should be deployed on the user's web browser (client-side) in order to protect sensitive user data from being skimmed or leaked from third-party tags

97% State a client-side protection and compliance solution to prevent sensitive data collection and data skimming would be valuable

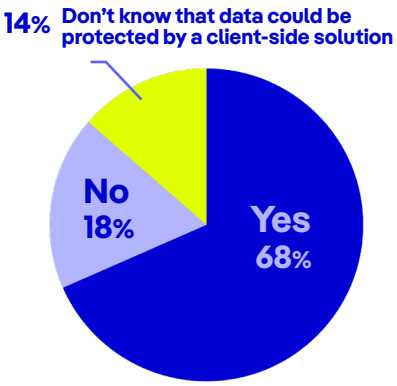
36% Have policies and tools to prevent digital skimming

The awareness of need is clear. 97% of respondents state a client-side protection solution to prevent sensitive data collection and data skimming would be valuable.

If a client-side protection and compliance solution were able to protect sensitive data from being skimmed or collected by third-party tags, how valuable would that be to your company?



That said, only 36% have policies and tools to prevent digital skimming.



In your experience, should a solution be deployed on the user's web browser (client-side) in order to protect sensitive data from being skimmed by or leaked to third-party tags?

While only 36% have policies and tools to prevent digital skimming, 68% agree that a solution should be deployed on the user's web browser (client-side) in order to protect sensitive user data from being skimmed or leaked from third-party tags. "Should be deployed" represents stronger language than "would be valuable.

The Bottom Line

In this digital economy, businesses increasingly benefit from their websites' use of third-party tags to deliver analytics, user tracking, payments, social media, communication, support chat or chatbots, performance measurement, and more. But companies aren't doing enough to protect themselves and their customers against cyber attacks. Again, only 36% have policies and tools to prevent digital skimming.

Organizations need to be able to ensure full client-side protection against digital skimming attacks and receive alerts about changes to these tags, forewarning potential data theft risks.

97% indicate they know that third-party tags collect sensitive information, but only 13% know exactly what data tags are collecting. At the same time, 49% admit that tags have collected data they weren't supposed to. Is it this 49% of respondents that believe there's really a problem?

More encouragingly, 68% of respondents agree that a client-side protection and compliance solution could protect user data from being collected, skimmed, or leaked by third parties. And, there is evidence that compliance is increasingly a driver, as 61% state that a tool that prevents digital skimming is key to achieving PCI DSS compliance.

Whether compliance or security is the driver, 97% indicate they know that third-party tags collect sensitive information. If that knowledge more often translates to doing more to make sure that this information is secure, then the industry is on the right path.

13%
Know exactly what data tags are collecting

68%
Agree that a client-side protection and compliance solution should be deployed to protect user data from being collected, skimmed, or leaked by third-parties

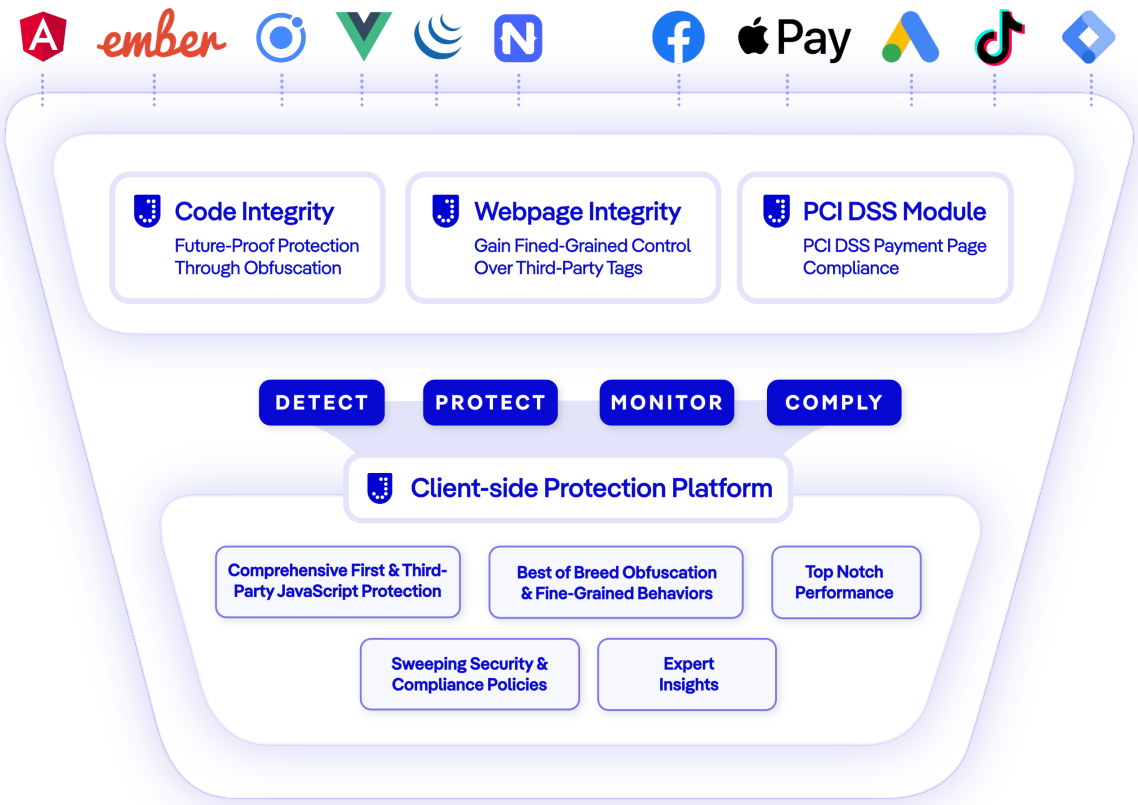
61%
State that a tool that prevents digital skimming is key to achieving PCI DSS compliance

Jscrambler Approach: Comprehensive Client-Side Protection & Compliance

What businesses need is a single integrated platform that enables them to adopt an end-to-end approach to client-side protection and compliance.

Jscrambler's unified Client-Side Protection and Compliance Platform ensures a robust defense against current and emerging client-side cyber threats, data leaks, and IP theft, data breaches, formjacking, web skimming attacks, compliance violations and data exfiltration by blocking unauthorized behavior while empowering software development and digital teams to innovate online securely with JavaScript, all without slowing down your website.

Jscrambler's solution covers every page, protects every user of the website, and safeguards all third-party tags and first-party JavaScript, across millions of users and their data.



All in all, the platform ensures a unique, comprehensive approach to safeguarding businesses from intentional or unintentional data leakage by competitors, third-party advertising and social media partners.

> ***"The Jscrambler platform is capable of streamlining the effort required to establish the effective application of controls and to lower the overall effort required to demonstrate and maintain compliance."***

Burke, M., Coalfire (2024). A Comprehensive Approach to Payment Page Security & PCI DSS v4.0 Requirements 6.4.3 & 11.6.1. [White paper]. Retrieved from here.

COALFIRE

About Jscrambler

Jscrambler is the leader in Client-Side Protection and Compliance and the first to merge advanced polymorphic JavaScript obfuscation with fine-grained third-party tag protection. With Jscrambler, businesses adopt a unified, future-proof client-side security policy all while achieving compliance with emerging security standards including PCI DSS v4. Jscrambler serves a diverse range of customers, including top Fortune 500 companies, online retailers, airlines, media outlets, and financial services firms whose success depends on safely engaging with their customers online.

If you want to know more about how Jscrambler can help you prevent client-side attacks, don't hesitate to contact us.

jscrambler.com/contact-us

CYBER SECURITY EXCELLENCE AWARDS WINNER 2023

50 Technology Fast 50 2023 PORTUGAL Deloitte.

Gartner HYPE CYCLE FOR APPLICATION SECURITY 2024

BIG INNOVATION 2024

G2 Highest User Adoption FALL 2024