source DEFENSE

Understanding Third-Party Risk in the Financial Services Digital Supply Chain

The Hidden Security and Compliance Gap That Could Cost You Millions

INTRODUCTION

If you were a cybercriminal, how would you go about attacking a financial services target such as a bank, credit card company, or brokerage? Would you spend the considerable time and effort needed to break the defenses of a hardened online or mobile banking application? Or would you instead look for a more readily exploitable vector like third-party and fourth-party plug-ins in use across nearly every financial services website?

Of course, you would choose the quickest route and the one that offers the greatest likelihood of success. Web properties across the financial sector rely on a rapidly expanding number of digital supply chain partners and suppliers for everything from payment services to data feeds, advertising to credit ratings. These third, fourth and nth party providers dramatically expand the attack surface for financial services.

While companies in this sector have invested considerable time and money in locking down their mobile banking applications, the company website is often perceived as less vulnerable given investments in server-side web security defenses. Unfortunately, nothing could be further from the truth. In fact, cybercriminals have learned that it is much easier to attack the website as it exists within a visitor's web browser, sometimes called the front-end or client-side of a web application.

Client-side attacks — including digital skimming, formjacking, clickjacking, ad injection, content defacement, and others represent some of the biggest third-party risks to security and compliance today. Traditional server-side security measures are ineffective against client-side attacks. This fact is starting to become more of a prevailing realization. From compliance regimes such as Payment Card Industry Data Security Standard (PCI DSS) now including focus on client-side security to industry analyst group Gartner stating that web application client-side protection will become a mainstream focus by 2023, the world is waking up to the fact that web security must be extended beyond the network edge.

Third-Party Hacks

> Third-party attacks pose significant risks to the financial industry due to our reliance on a myriad of providers and suppliers. … 2021's successful attacks against third-party providers demonstrated that a one-to-many compromise chain is possible. Supply chain threats will undoubtedly persist, especially to target entities who are considered adequately hardened to traditional attack methods, such as financial institutions."
>
> **— "Navigating Cyber 2022," Financial Services Information Sharing and Analysis Center (FS-ISAC)**

THE GROWING RELIANCE ON THIRD AND FOURTH PARTIES

As a financial services organization, you can control first-party risk through governance and the defenses you put in place against attacks. Your organization can control second-party risk (your customers) by encrypting their sensitive data. The problem your company and others in the financial sector face today is how can you mitigate the growing third-party (fourth-party and nth-party) risk in your digital supply chain?

As digital transformation grows, financial service companies are embracing a wide variety of third-party functionality that enhances and extends the customer experience — within their web browser — such as payment platforms and services, analytics, data and news feeds, advertising, and more. Third-party scripts often source additional content and functionality from fourth parties, further extending the web application's supply chain. And those fourth-party scripts can source additional content from virtually anywhere.

All of which means that the average financial services web application has a significant amount of code being sourced from third, fourth and nth parties — placing it outside of the control of the company. This code effectively negates any

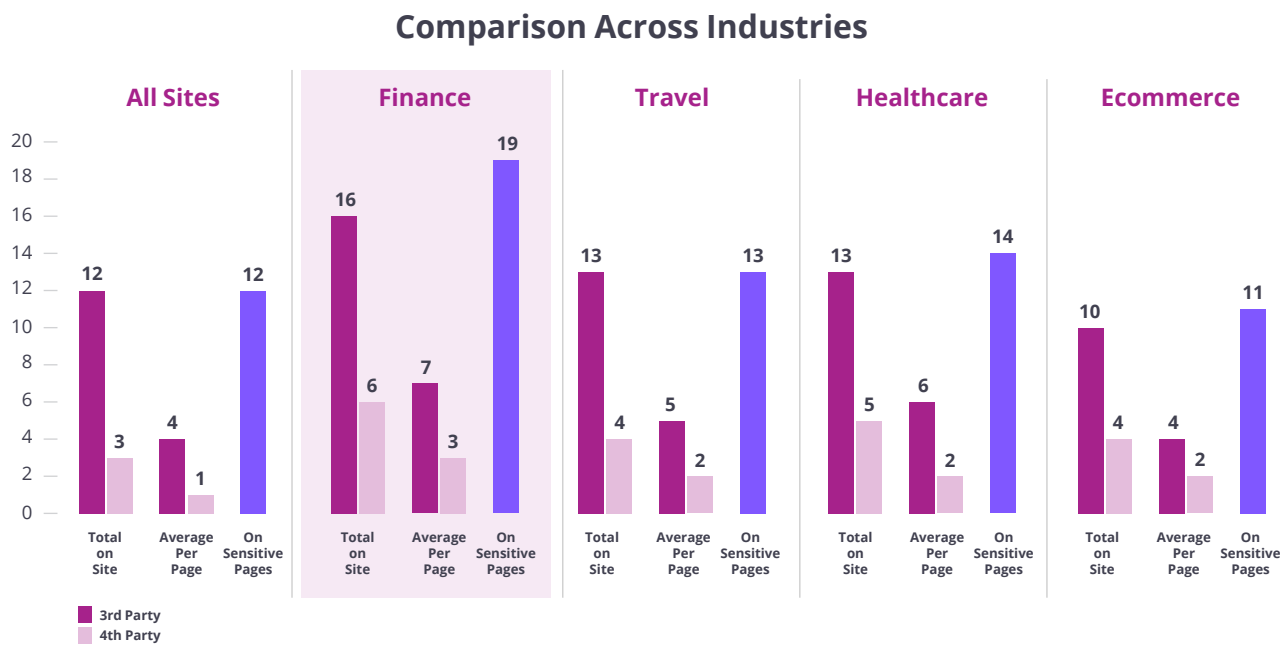
attempt to implement a zero trust security model, and represents a real and present danger to both security and compliance.

According to a Source Defense website analysis of the top 4,300 websites by traffic around the world, the average number of third-party scripts in use is 12 and on the average website, 12 third- and fourth-party scripts appear on at least one sensitive page, such as a login and credential capture page.

The analysis shows that the financial services industry has significantly more third-party and fourth-party scripts on their websites than the other industries reviewed, with an average of 16 third-party and 6 fourth-party scripts. Worse yet, the financial services websites have 58% more scripts running on sensitive pages than the average across industries (19 in financial services versus 12 across industries), see Figure 1.

These services all reside and operate outside of your security team's control because they are loaded from third-party and fourth-party servers directly to your customers' browsers. This creates a material security risk that cannot be addressed using traditional server-side security measures.

Figure 1: Third- and Fourth-Party Scripts Found on Websites Across Four Major Industries



THE JAVASCRIPT VULNERABILITY THAT MAKES THESE ATTACKS POSSIBLE

Unlike exploitation of a newly discovered vulnerability, cybercriminals are taking advantage of a long-known security flaw in JavaScript that gives all scripts — regardless of the source — the same level of control on the client-side. This means that any JavaScript code, including third-party and fourth-party code, has full access and authorship capabilities, which enables access to any and all data in forms, such as customers' personal and financial information.

Here's how cybercriminals take advantage of this to attack financial services companies:

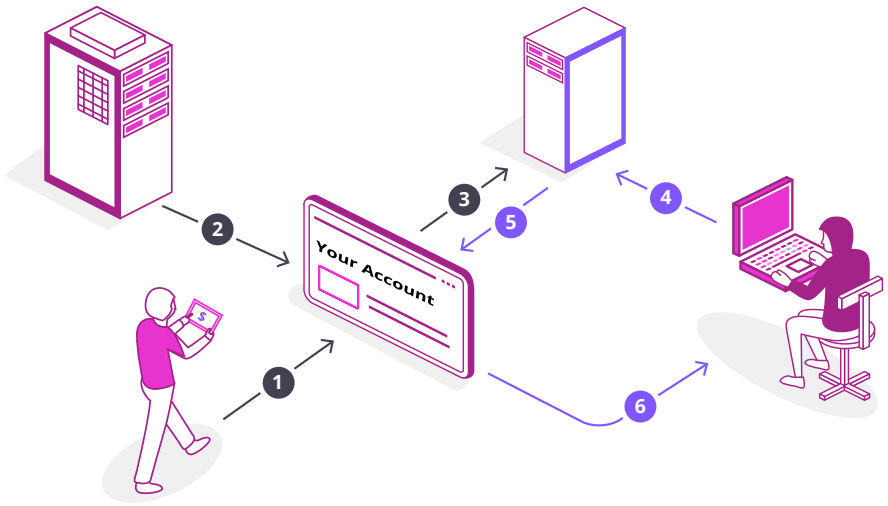
- Content is served and enriched: Front-end web application logic — a combination of the financial services company's application code and the integration of third-party content and functionality — is loaded and runs on the client-side in the browser, beyond the protection of server-side security. The code is dynamically downloaded from a remote server, which means that it bypasses the traditional security infrastructure, including the company's firewalls and web application firewalls (WAFs).

- All scripts have the same level of control: Third-party and fourth-party scripts have the identical level of control as the financial company's own script. Every script on the page, no matter its origin, has access and authorship capability, meaning it can change the webpage, access all information on it (including forms), and can even record keystrokes and save them.

- The vulnerability is easily exploited: No component of traditional security programs can prevent client-side attacks perpetrated via JavaScript. All it takes is for the third-party vendor to be hacked and have its code changed or an internal developer to integrate malicious code, whether accidentally or intentionally. Financial services companies have limited means to dynamically detect the change and no means using server-side security solutions to prevent it from exfiltrating data or executing other malicious activity from the customer's browser.

Nearly every web application (97.9% of all websites) in the world uses JavaScript as its client-side programming language[1] — making these types of attacks one your company's biggest cybersecurity gaps.

Figure 2. Client-Side Web Application Attack



1. An investor visits a brokerage website.
2. Content is presented in the investor's browser from the corporate web server.
3. The content is enriched with third-party JavaScript.
4. An attacker compromises the third-party server.
5. Malicious content is served to the investor's browser.
6. The attack is successful. Customer data is exfiltrated, putting compliance and brand integrity at risk.

1. "Usage Statistics of JavaScript as Client-Side Programming Language on Websites," W3Techs, February 2022

WHY CURRENT SECURITY MEASURES ARE NOT ENOUGH

Traditional server-side security does not address these JavaScript risks because client-side scripts operate completely outside of the security capabilities an organization deploys to secure the server side of their web applications.

Other security measures that may already be in place fall short as well. Application security validation testing or dynamic application security testing are not designed to test every use case or operate dynamically, nor can they test the code residing on third-party or fourth-party remote servers. They are also not capable of providing real-time scanning of all web traffic across the entire user population.

Likewise, using content security policy (CSP) and/or subresource integrity (SRI) features are not enough to protect client-side web applications from today's threats. While CSP and SRI can be powerful tools for website protection and data management, they have significant limitations that impact the ability for website owners to use these measures effectively against client-side threats.

Because it's difficult or impossible with existing security tools to detect these attacks, the majority aren't discovered for weeks or months, increasing the scope of damage and mitigation costs significantly.

THE DANGERS OF UNDERESTIMATING THIRD-PARTY RISK

For the first time, Financial Services Information Sharing and Analysis Center's (FS-ISAC's) regional Threat Intelligence Committees (Americas, EMEA, APAC) raised Cyber Threat Levels an unprecedented three times in one year due to supply chain incidents, including major third-party threats, with potential impact on the financial sector. The association does not see these trends subsiding as businesses continue to digitalize.[2]

The growing awareness of third-party risk within the financial services sector extends to regulators as well. Financial regulators around the world have begun to issue more stringent guidance on third-party risk management and operational resilience. From the U.S. Securities and Exchange Commission to the European Central Bank to the Monetary Authority of Singapore, authorities have signaled they plan to increase cybersecurity compliance obligations including holding firms accountable for service providers' cybersecurity measures.[3]

Financial services companies are already held responsible for protecting consumer data and privacy via regulations such as the General Data Protection Rule (GDPR) and the California Consumer Privacy Act (CCPA). Third-party threats that result in a breach of personal customer data can result in significant regulatory fines and penalties, not to mention the impact on customer trust.

2. "New FS-ISAC Program Boosts Supply Chain Security Dialogue," Devon Warren-Kachelein, InfoRisk Today, January 2022
3. "Global Cyber threats to Increase in the Financial Sector," Tilly Kenyon, Cyber, March 2022

A data breach or leakage can also incur other direct costs such as legal fees, settlements of lawsuits, damages, forensic investigation, audit, and remediation. Ally Bank faces a proposed class-action lawsuit over data leakage that exposed customer information to third-party business partners through a website programming error.[4] Indirect, but not insignificant, costs include brand reputation loss, customer churn, and downtime — all of which can impact revenue, company valuation, stock price, and shareholder value.

Today the average cost of a data breach is $4.24 million, up from $3.86 million in 2020. The financial services industry has the second highest average total cost of all industries at $5.72 million. More than one-third of the costs (38%) are lost business, including customer turnover, lost revenue due to system downtime, and the cost of acquiring new business due to diminished reputation. The loss of customer personally identifiable information (PII) results in an average cost of $180 per lost or stolen record.[5]

4. "Ally Bank Hit With Class Action Over April 2021 Data Breach," Erin Shaak, ClassAction.org, December 2021
5. "Cost of a Data Breach Report 2021," Ponemon Institute and IBM Security, July 2021

Breach Exposed Personal Data of More Than 100 Million Customers

A data breach at Capital One bank resulted in an $80 million fine and the company settled a class-action lawsuit filed by customers for $190 million.

Source: "Capital One Settles a Class-Action Lawsuit for $190 Million in a 2019 Hacking," Lananh Nguyen, *The New York Times,* December 2021

HOW FINANCIAL SERVICES COMPANIES CAN PROTECT CLIENT-SIDE WEB APPLICATIONS

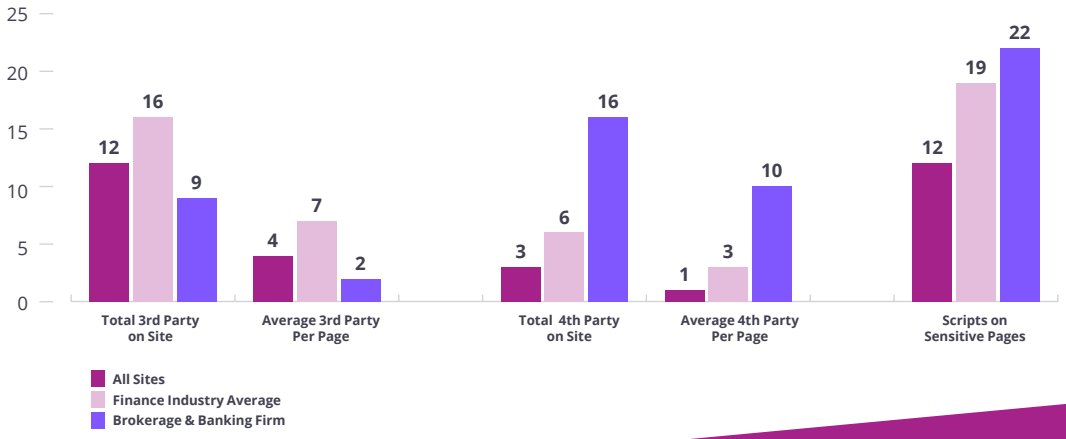
With adversaries increasingly focused on the client-side, financial services companies must give equal attention to reducing the large material risk inherent in the JavaScript attack vector.

The best place to start is to gain a deeper understanding of your company's digital supply chain. For example, Source Defense analyzed the website of a leading U.S. brokerage firm and compared the findings with those in the financial services industry as well as the average across all industries for more than 4,300 websites.

Compared with both the overall and finance industry averages, this firm uses significantly fewer third-party scripts, both in total and on each page. However, the firm's website includes many more fourth-party scripts. The total number (16) is five times the overall average (3), and more than double the finance industry average (6). The average page on its site has 10, which is an order of magnitude more than the overall average, and more than three times the finance industry average.

The data also shows more third- and fourth-party scripts on sensitive pages (22) than either the overall average (12) or the finance industry average (19). This also indicates a higher than typical exposure to risk.

Figure 3: Third- and fourth-party scripts for the example brokerage and banking firm versus overall and finance industry averages



While there may sound reasons why this organization's website includes so many scripts, the security team should investigate further to understand:

- Why are there so many fourth-party scripts?
- Could the number of scripts be reduced?
- Could some scripts be removed from the pages that handle sensitive information?
- Does the firm need to invest more in tools or people to assess and monitor these scripts?

The next step is to deploy a solution specifically designed to provide client-side web application protection using a prevention-first approach versus only a detect-and-alert approach. With most security teams already overworked, understaffed, and drowning in alerts, solving the client-side problem can't add more burden for the security team. Solutions relying on a detect-and-alert approach flag potentially malicious activity and ask the team to investigate and respond to what can be thousands of false positives.

Instead, your company needs a solution that prevents the problem from the start, doesn't impact site performance, and requires little to no human oversight to work.

DETECT, PROTECT, AND PREVENT CLIENT-SIDE ATTACKS WITH SOURCE DEFENSE

As the leader in web application client-side protection, Source Defense delivers what many might believe to be a unicorn in cybersecurity — a solution that is simple to deploy, has a management burden of a mere few hours per month, and adds no additional burden on already overburdened security teams.

Source Defense is a prevention-first technology that stops the threat of client-side attacks without the need for alerts and investigation by security staff. Source Defense already secures nearly one billion transactions and prevents nearly two billion compliance policy violations per month for some of the world's largest companies. The Source Defense patented Website Client-Side Security Platform offers the most comprehensive solution to detect website skimming, formjacking, and supply chain attacks and stop them before they affect your website or your customers.

Source Defense uses real-time, client-side sandboxing and permissions-based isolation and reflection to protect your company and your customers' data and prevent successful data exfiltration or leakage by:

- Isolating and monitoring JavaScript execution in an end user's browser, in real time, as the user interacts with your web page
- Using real-time JavaScript sandboxing to restrict the access that each script has to a web page as well as control that script's behavior
- Allowing or restricting access to different parts of the page and the data that they contain
- Monitoring and managing the flow of data from the page to other places
- Enforcing security controls

CONCLUSION

The financial services industry has always been a prime target for cybercriminals. As the move to online banking and financial services continues to accelerate, security teams have focused on locking down applications to protect the organization and its customers.

Unfortunately, the same security measures don't work to protect your business and customers from client-side attacks on your web applications. That's why banks, brokerages, insurance firms, and others in the financial services sector should adopt a solution that specifically prevents client-side attacks from being successful.

Source Defense offers the only purpose-built, patented technology for real-time protection against risks and threats originating in JavaScript.

To learn more, visit
https://sourcedefense.com/request-a-demo/

To see how your website stacks up against threats and understand your risk, request a free risk report by visiting
https://sourcedefense.com/check-your-exposure/

source
DEFENSE

About Source Defense

Source Defense is a security, compliance and performance optimization platform for any website that collects sensitive data or is transaction oriented. As the market leader in web application client-side protection, Source Defense addresses a ubiquitous gap in the management of 3rd party digital supply chain risk with a zero-trust model that extends security beyond the network to the edge/client-side. The Source Defense Platform provides real-time threat detection, protection and prevention of vulnerabilities originating in JavaScript, and currently protects leading organizations in the financial, healthcare, hospitality, and retail markets from the threat of JavaScript based attacks such as Magecart, digital skimming, credential harvesting and click-jacking. Source Defense secures nearly one billion transactions and prevents nearly two billion compliance policy violations per quarter.