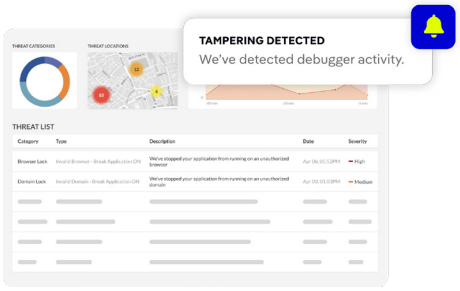
jscrambler

# Jscrambler Solution for Financial Services

Protect your web banking applications from fraud and data leakage while achieving compliance with regulations. Keep innovating while making sure no attacks come through third-party tags and pixels.




Financial institutions use JavaScript to develop highly advanced banking platforms. However, JavaScript is exposed and opens the door to client-side attacks that average **$2.5M annually**. **44%** of organizations with annual revenue of less than $1 billion were unable to recover funds lost due to payment fraud attacks*. One instance of transaction fraud, malicious interface changes, or magecart-style data breach can cost millions and damage reputation. For example, one trojan attack cost Citadel **$500M.**

* according to Payments Fraud & Controls Report JP Morgan (2023).

## Jscrambler's Client-Side Protection Platform mitigates the threats to web banking platforms

### Protect your Intellectual Property

Get warnings if your JavaScript code is being debugged, tampered with, or being used outside your desired environment.

### Maintain stellar data protection standards

Prevent access and transfer of data inserted into forms by blocking script misbehaviors with fine-grained control of their actions and their level of access.

### Mitigate financial and reputational risks

Efficiently protect native code and thwart potential threats coming from third-party tags and pixels. Leave no room for data breaches.

## Top features to help you secure your banking platforms

**Banking Application Shielding:** With polymorphic obfuscation, code locks, and runtime protection, attackers won't be able to reverse engineer, debug or tamper with the code of your web/mobile app.

**Real-time Threat Notifications:** Get warnings when your JavaScript code is being debugged, tampered or stolen, enabling you to immediately take any supplementary actions.

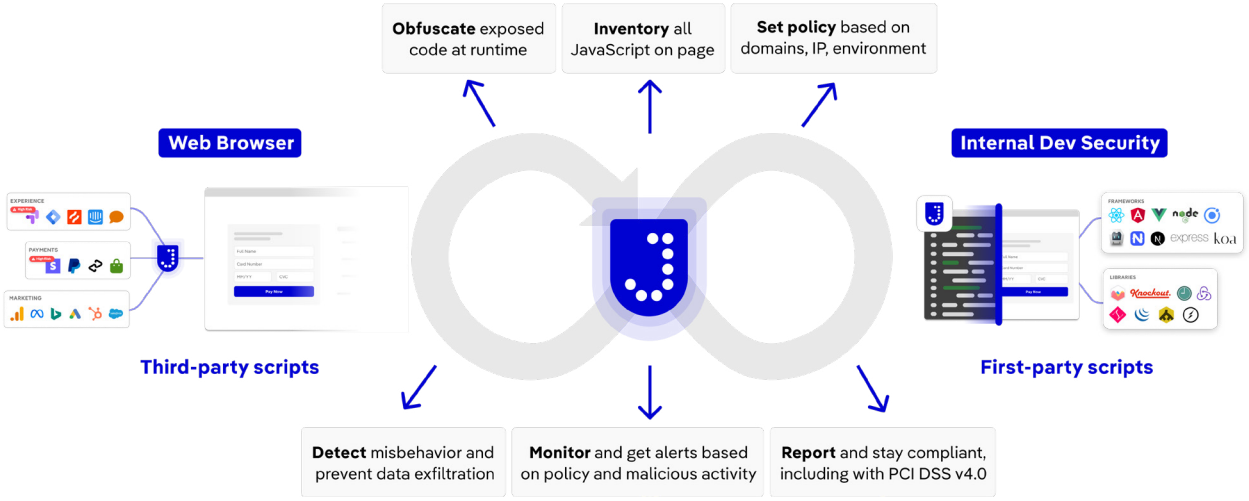
**Third-Party Management:** Jscrambler's monitoring agent runs in every user session, in real-time, regardless of the user's device and browser. It detects suspicious outbound network events like Magecart and data exfiltration.

**Webpage Threat Mitigation:** Powerful and granular rules engine that provides full control of each script running on your website. Allows proactively or reactively blocking scripts that exhibit malicious behavior.

**Compliance with Regulations:** Proactively manage how data is accessed and transferred on the client side to better comply with regulations like PSD2, PCI DSS, GDPR and CCPA.

**"Jscrambler fulfilled the entire checklist of the application security worries we had".** CTO at MeDirect

## Jscrambler is the most comprehensive solution for client-side protection




## Trusted by the leaders in their industries

Jscrambler's technology is trusted by many of the Fortune 500 and thousands of companies globally.

**Companies we serve:**

- 25+ Major banks worldwide
- Top 3 entertainment companies in the US
- Leading companies in E-commerce, Financial Services, Broadcasting, and IT
- A major airline in the EU
- Top retailer in the US

### About Jscrambler

Jscrambler is a leading authority in client-side security software. Its solution defends enterprises from revenue and reputational harm caused by accidental or intentional JavaScript misbehavior. Jscrambler was recently recognized as a winner in the 2023 BIG Innovation Awards.

If you want to know more about how Jscrambler can help you prevent client-side attacks, don't hesitate to contact us.
**hello@jscrambler.com | +1 650 999 0010**