PSD2 – Control screen scraping access

PSD2, the revised Payment Services Directive took effect in January 2018 to bring open banking to Europe. The directive aims to trigger competition, innovation, and increase customer protection in the European payments industry.

Under the new directive, financial institutions (FIs) are required to share customer data with compliant aggregator services via open APIs. Because of this new open architecture, aggregators will no longer be allowed to access customer information from payment accounts using screen scraping techniques.

For the first time, the new directive provides aggregators with a clear entry point to access customer data, as an alternative to screen scraping.

What does this new landscape mean for financial institutions?

NuData Security

mastercard

Screen scraping in short

Screen scraping is the automated use of a web environment to extract data. This technique extracts personal customer data or performs actions that would otherwise be manually made by the customer.

Screen scraping is commonly used by aggregators to offer customers third-party services in the financial technology space.

Where does the screen scraping risk come from?

Screen scraping can pose a risk for customers and FIs because:

- Although legally not permitted, aggregators can collect more customer information than they are entitled to.
- It is challenging for institutions to determine if the aggregator is a legitimate partner or if it is a fraudulent interaction that should be mitigated.

Controlling screen scraping

With the new directive, PSD2 wants aggregators to leave a clear trace of their actions in an environment. To achieve this, aggregators will no longer access customer payment accounts via screen scraping. Instead, FIs are required to grant aggregators, and other third parties, access to these accounts via dedicated interfaces. By using a dedicated interface, the aggregator has to identify itself and leave a clear trace of its actions. This ensures that the aggregator only collects the expected sensitive customer data – protecting customer information.

Does this mean the end of screen scrapers?

No. During the PSD2 transitional period, screen scraping is still allowed. The ban on screen scraping won't go into effect until September 2019. However, after that date, aggregators can continue to use this technique illegally, threatening your customer's data and trust.

NuData Security
mastercard

Yes; you can say no

Now FIs can reject illegal screen scraping attempts and protect their environment. Financial institutions that have the right security in place can detect unlawful activity and block it. This gives institutions the opportunity to protect their customers and strengthen those relationships. With a safer digital environment, financial institutions can provide innovative digital solutions without fearing illegal activity.

Block unwanted screen scraping

NuData's flagship product, NuDetect, combines different layers of intelligence, including behavioral biometrics and intelligent automation detection, to give the power back to the financial institutions. Businesses can detect unwanted traffic and mitigate the risk in real time.

How can you control screen scraping?

Choose your best NuData option to protect your customer's data

1. **Block all**
   End all screen scraping activity on your site. *See case study on the next page.*

2. **Block some**
   Chose what aggregators you want to let into your environment during the transitional period and keep the rest out.

3. **Automated account takeover detection**
   Identify account takeover attempts within the screen scraping activity while you allow valid users to continue their session.

"NuData stopped millions of automated login attempts that our previous solution had missed." Major U.S. bank

NuData Security
mastercard

"NuData uniquely secures faster payments while still offering a great experience." Early Warning

Compliance and trust

As part of Mastercard's layered approach to payment security, we help your financial institution build trust during the PSD2 transitional period. We can do this currently, while screen scraping is allowed, as well as in the future when screen scraping on payment accounts is banned. NuDetect provides a trusted solution to protect customers today and tomorrow.

Who is NuData Security

We are an award-winning Mastercard company that offers enhanced online verification through user device interactions, including passive biometrics. Our unique solution, NuDetect, uses cutting-edge technology such as behavioral analytics, device and connection detection, and machine learning capabilities to accurately identify who or what is accessing your environment with near 100% accuracy.

Our solution identifies machines from humans, then separates good machines from bad and selects known humans from unknown humans.

With over 200 billion events analyzed per year, we are trusted by major global brands to protect their environment from sophisticated, mass-scale automated attacks.

NuDetect also protects you from:

- Server scripting
- Client browser or app scripting
- Client browser manipulation
- Native app spoofing
- Enterprise API scripting
- Device identification and spoofing

Our proven track record

A Top 10 U.S. Bank using the Block All service

During a 90-day period:

250M
unwanted aggregator login events blocked

+99.9%
accuracy rate

0.1%
false positive rate

NuData Security
mastercard

Talk to your Mastercard Representative
Email us at bizdev@nudatasecurity.com
Visit www.nudatasecurity.com