MANAGING BOTS IN
FINANCIAL INSTITUTIONS

For many financial institutions, traffic from bots (aggregators, scrapers, crawlers) can account for up to 40-60% of their overall website traffic — from good bots engaged in essential business tasks to bad bots performing harmful activities. Banks, traders, asset managers, and insurers might know how much of their traffic is from bots, but what they may not know is the impact those bots may be having on their business.

Bots are an essential part of our Internet ecosystem. However, bot traffic can reduce website performance for legitimate users and increase IT costs. To address this, financial institutions need a flexible framework to better manage their interaction with different categories of bots (aggregators, scrapers, crawlers) and the impact bots have on their business and IT infrastructure.

Financial Data Aggregators

Financial account aggregators compile information from different bank accounts, investment accounts, credit card accounts, and other consumer or business accounts. Account data is gathered by means of direct data connections or "data scraping," where a user provides the account-access information allowing an automated system to "scrape" or gather the information from an interface designed for humans. Aggregators are popular and are designed to help people better manage their money by reducing the time-consuming work of gathering and manually entering data. Additionally, aggregators can eliminate the need to transfer copies of statements, and provide a comprehensive view of a client's net worth, including investments, assets, and liabilities. But, many financial institutions are looking for greater control over the growing volume of traffic coming to their site from these account aggregators. Aggregators can generate performance issues caused by the concentration of users accessing the content simultaneously. Additionally, financial institutions want to be able to track the human vs. bot traffic, reduce risk, and ensure reliability of their digital properties.

How Customers Find a Financial Institution's Site: Financial customers today are searching for, performing research on, and often signing up for new financial products through a digital channel. The first step is to conduct an online search (e.g., Google, Bing, Yahoo!). Bots play an important role here. Search engines create bots to crawl websites, and return information on a site's content, and help shape how those websites are prioritized in search results. Online banks, investors, and insurers must ensure high website performance for search-engine crawlers as well as users, because slow site load times can negatively affect rankings and user experience.

Some big banks have resorted to cutting off non-partner aggregators by keeping their data off limits. This decision can be unpopular with consumers, who expect to be able to easily and accurately view all of their financial information in one place — enabling more informed financial decisions

Another role aggregators, or bots, play with financial services institutions is to crawl their site to evaluate the effectiveness of their SEO efforts. This can be done via bots created internally or via a third-party service. While this is a necessary and important business need, financial institutions must ensure that these bots get the information they need without negatively impacting their customer's digital experience.

How Bots Affect the Digital Experience: Today's financial services customers are influenced by their daily interactions on social media and other platforms, expect all digital experiences to be high performing and lightning fast, and have limited tolerance for slow page load times. However, with up to 40-60% of traffic being bots, too many bots operating too freely, regardless of the type or intention, will result in a degradation of website performance, causing legitimate, human traffic to have a negative experience, which can lead to site abandonment and subsequently, customer churn.

Content Personalization: Optimizing customer experience and new customer acquisition tactics requires a holistic understanding of the user. Financial institutions can leverage advanced marketing analytics tools to gain greater insight and provide relevant information to customers and prospects, uniquely tailored to their specific needs. This, in turn, enables them to deliver a more customized user experience, leading to more satisfied customers and better customer retention as well as more new customers. However, a by-product of the proliferation of bot traffic is that marketing data, which drives key tactical and strategic decisions, can become polluted, including both legitimate human activities, and bot activities. Bots skew the data and misrepresent the true nature of a financial institution's customers, invalidating conclusions drawn from the data set.

Competition: Mortgage and other loan rates, investor relation information, and trading data are all critical to a financial institution's ability to attract and retain customers. Competition can use bots to regularly and automatically crawl the financial institution's site to "scrape" this data for competitive advantage. Financial institutions also need to manage third party aggregators that crawl the sites of multiple financial institutions for interest rates and then present them on a third-party site, potentially enticing customers away.

What does good look like?

The ideal solution would allow financial institutions to manage bot traffic to ensure the best possible outcome — maximizing the positive results and minimizing the negative — depending upon the type of bots they see.

For example, while you want to allow good bots to do their job, there are circumstances where they may need to be ratcheted back to ensure the human web traffic can access their accounts without issue.

When a financial institution encounters bad bots, blocking them is only a temporary solution, which can be ineffective in the long run; blocked bots will simply return smarter and faster. By managing how those bots are allowed to interact with the site, you can minimize the negative impact of those bots without tipping off the operator that you are on to them. Two common solutions are simply slowing them down to reduce the value and timeliness of the information they are gathering or serving them alternative information such as pushing them to a page with intentionally inaccurate content.

Akamai's Bot Manager: In direct response to the current state of bot solutions, Akamai has created a unique alternative for financial institutions struggling to deal with the bot problem. The solution is designed to allow financial institutions to identify, categorize, and manage the bots — both good and bad — to achieve the goals for their website. Akamai's Bot Manager provides a range of management actions beyond just blocking to help financial institutions maximize the positive and minimize the negative impacts of their bot traffic. They are then able to analyze and report the activity to improve visibility on the bot issue. In addition to visualization and reporting on bot traffic, Bot Manager can also help organizations with their own internal marketing data. Website and page-view statistics can be significantly skewed by bot traffic, making it difficult to understand the behavior of real users interacting with the site. Akamai's Bot Manager identifies bot-generated requests in order to filter out bot traffic from human traffic, which can help improve marketing's data and analysis, and lead to better business decisions.

To learn more about Bot Manager visit us here.

Akamai FASTER FORWARD