What a Tracking Technology Class Action Lawsuit Can Teach Financial Institutions

Banking Brief: Financial Services Insights

By Patrick Mastrian III and Larry Tomlin on May 20, 2025

Financial institutions that use code-based tracking technologies may soon find themselves facing increased scrutiny and legal exposure as the next wave of class action litigation begins.

On December 19, 2024, a member of Everwise Credit Union initiated a class action lawsuit alleging the credit union disclosed his sensitive personal and financial information to various third parties without his knowledge or consent.

The case underscores the importance of transparency and consent in the handling of personal and financial information.

The Complaint Against Everwise: Nonpublic, Personal Information Shared

According to the complaint, Everwise employed code-based tracking technologies on its website that collected and transmitted a wide array of nonpublic personal information and personally identifiable financial data of its members. These tools allegedly captured detailed records about the members' online activity, including, but not limited to, membership and vehicle loan application information, credit card application details, the applicants' first and last names, email addresses, purposes for seeking credit, account funding methods, driver's license information, and co-applicant details. The tracking technologies also reportedly recorded user behaviors on the website, such as which pages were visited, which buttons were clicked, and the destinations of those clicks.

The member further claimed that Everwise failed to provide any meaningful notice that this information was collected and shared with third parties. More concerningly, the member alleged these third parties were permitted to pass along the collected information to additional entities, referred to as "fourth parties" in the complaint, without the member's knowledge. At no point, according to the complaint, were members informed of this practice, nor were they offered a genuine opportunity to opt out of the data sharing.

Best Practices for Handling Consumer Data

If any financial institution uses code-based tracking technologies on its website that mines data similar to the allegations in the Everwise litigation, exposure under the Gramm-Leach-Bliley Act and potentially state consumer protection statutes may result.

In light of this emerging litigation risk, financial institutions and other organizations that handle consumer data should consider implementing the following precautionary measures:

1. Conduct a thorough review of all customer-facing web applications and tracking technologies to confirm compliance with privacy standards;
2. Remove or disable any technology that transmits personally identifiable or financial data without explicit customer consent;
3. Implement clear disclosure and consent protocols before any data is shared with third parties;
4. Adopt technical safeguards that actively prevent unauthorized transmission of sensitive information via tracking software; and
5. Utilize strong indemnification language in the vendor contracts with technology companies to protect your institution from unauthorized data mining.

Proactively addressing these issues can help mitigate legal risk, maintain consumer trust, and demonstrate good faith compliance with applicable privacy laws.