Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

Website Pixel & Tracking Technology Litigation

SUMMARY

Financial Institutions are increasingly being targeted by class-action lawsuits alleging that website tracking technologies, such as Meta Pixel, Google Analytics/Google Ads, LinkedIn Insight Tag, cookies, session-replay tools and other third-party scripts, improperly transmit information about website visitors to third parties without adequate consent.

Plaintiffs are increasingly relying on state wiretap/eavesdropping laws, including California's Invasion of Privacy Act, as well as other privacy statutes. Importantly, compliance with GLBA and Regulation P does not necessarily eliminate this litigation risk.

Ask yourself; **"Can we demonstrate exactly what information our website tracking technologies collect, where that information goes, what third parties receive it, and what consent or legal basis permits the collection and disclosure?"**

If the answer is **"we don't know"**, you should consider the issue an immediate risk-management priority.

HIGH-RISK AREAS

Pay particular attention to tracking technology operating on:

- Loan, mortgage and HELOC pages
- Credit card and debit card pages
- Online account opening pages
- Loan/application forms
- Financial calculators
- Member login or authenticated areas
- Pages revealing a consumer's financial interests or circumstances
- Pages containing forms, chat, videos or other interactive features

RECOMMENDED MITIGATION STEPS

- **Inventory every tracking technology** operating on the public website, including technologies installed by marketing agencies or website vendors.
- Identify **every third-party receiving website data** and determine exactly what information is transmitted.
- Determine whether tracking begins **before affirmative user consent.**
- Determine whether URLs, IP addresses, cookies, clicks, page metadata, search terms, form information or other identifiers are transmitted.
- Review whether tracking technology is present on **loan, mortgage, HELOC, credit-card or other financially sensitive pages.**
- Review tracking technology in any **authenticated/member area.**
- Compare actual data collection against the credit union's **privacy notice and website disclosures.**
- Have legal/privacy counsel evaluate applicable **state wiretap, privacy and consent laws,** particularly for visitors from states where the credit union has no physical presence.
- Require vendors and marketing agencies to disclose all tracking technologies and obtain approval before adding new scripts.
- Review contracts for **indemnification, privacy obligations, data-use restrictions and notification requirements.**

Do not assume that a tracking pixel is harmless simply because it is commonly used or because it is provided by Google, Meta or another reputable vendor. Courts are increasingly allowing these cases to proceed, and the legal landscape remains unsettled.

The safest approach is to identify unnecessary tracking technologies, minimize the data collected, prevent sensitive financial information from being transmitted to third parties, implement appropriate consent mechanisms, document the credit union's decisions, and obtain legal/privacy review.

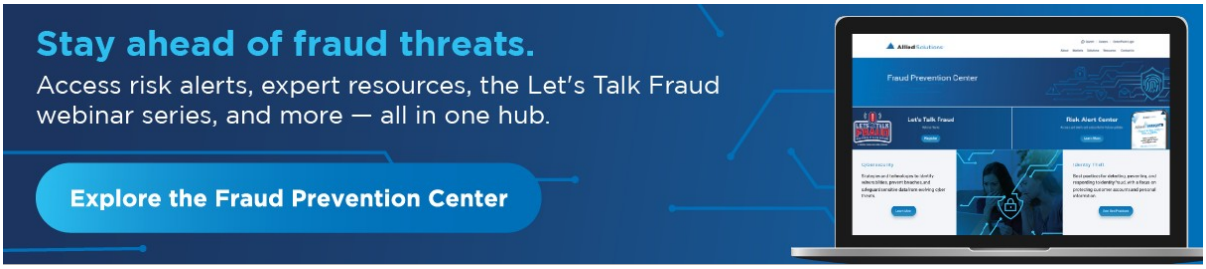
RISK MITIGATION RESOURCES

- NIST Privacy Framework
- Federal Financial Institutions Examination Council

- NCUA Website Privacy Policy
- Federal Trade Commission – Bringing Dark Patterns to Light
- California Privacy Protection Agency
- Visit our Fraud Prevention Center to learn best practices on protecting against website pixel and tracking technology

Need assistance or want to request a consultation?
Contact our risk specialists at risk_specialist@alliedsolutions.net

The information presented in this email is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this email.



LinkedIn