KRIEG DEVAULT

Insights

Financial Institutions Use of "Meta Pixels" Targeted in Latest Class Action Trend

January 13, 2025

By: Brett J. Ashton, Kay Dee Baird, David A. Bowen, and Scott S. Morrisson

Many financial institutions use the services of technology companies like Facebook or Google to track and record customer interactions with their website through the use of Meta Pixels, Internet Cookies, or other tracking technology to continually improve the ways in which they service their customers, and target products and services to those who most want and need them. While this practice benefits the consumer a number of class action lawsuits have been filed in recent years, initially against health care providers, alleging that this technology results in the company itself violating state and federal privacy or consumer protection laws.

Predictably, the plaintiff's bar recently began to adapt these cases to target financial institutions. As was the case for overdraft and NSF class action litigation, larger financial institutions were initially targeted, with claims filed against TD Bank, Barclays Bank, and Capital One Bank.[1] However, a recent class action against a much smaller Indiana based financial institution should cause all banks and credit unions to take note of the potential risks associated with the use of website tracking technologies.

These Meta Pixel cases typically assert a variety of claims based on alleged violations of contractual, common law, and statutory duties. Plaintiffs typically allege that the financial institution surreptitiously imbeds website tracking software created by various technology providers (including Meta, Google, HubSpot, and others) that records the consumers actions on the website, and then impermissibly transmits that data to the third party technology company. Complaints against financial institutions to date have included state law claims of negligence, negligence per se, breach of contract, unjust enrichment, bailment, conversion, violations of state privacy and wiretap laws, and violations of various federal laws, including the Gramm Leach Bliley Act ("GLBA"), Electronic Communications Privacy Act, Section 5 of the Federal Trade Commission Act ("FTC Act"), and the Computer Fraud and Abuse Act. While the GLBA and FTC Act do not provide for a private right of action, plaintiffs assert that the transmission of website tracking data to third parties constitutes a per se violation of each act, and the basis for a state law claim of negligence per se.

Key Takeaways

Financial institutions should immediately review their existing privacy and website disclosures to ensure they adequately disclose their use of Meta Pixels, Internet Cookies, and any other website tracking technology. While we

believe the underlying claims in these Meta Pixel cases are meritless, the stronger your disclosure processes the easier it will be to defend against these claims in the event your financial institution becomes the next target of the plaintiff's bar.

[1] See *Shah v. Cap. One Fin. Corp.*, No. 3:24-cv-05985 (N.D. Cal. 2024); *Stevens v. TD Bank NA*, Ct.Case No. 1:24-cv-08311 (D.N.J. 2024); *Vargas v. Barclays Bank Delaware*, Case No. 1:24-cv-06549-LGS (S.D.N.Y. 2024).

Disclaimer: The contents of this article should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult with counsel concerning your situation and specific legal questions you may have.