When “Just Send the Records” Isn’t Simple: Lessons from the FTC’s Amazon FCRA Settlement

Laura Riposo VanDruff, Donnelly L. McDowell

July 1, 2026

The Fair Credit Reporting Act (“FCRA”) is often thought of as a credit-reporting statute, but its reach is far broader—and its compliance demands far more nuanced—than many businesses may appreciate. The FTC’s recent settlement with Amazon regarding how companies respond to consumer requests to access transaction records in connection with potential identity theft illustrates this point.

Narrow Duty with Broad Consequences

The Amazon settlement relates to Section 609(e) of the FCRA, 15 U.S.C. § 1681g(e), which requires a business that has potentially transacted with someone who fraudulently used a consumer’s identity to provide the identity-theft victim with the application and business transaction records of the fraudulent transaction. The statute permits a business to require proof of identity and proof of the identity-theft claim, and it allows a business to refuse the request only in narrowly defined circumstances.

According to the complaint, Amazon routinely declined to furnish identity-theft records, citing “security” or “privacy” grounds that the statute does not recognize as valid bases for refusal. The complaint alleges that consumers were forced to navigate a “Kafkaesque” loop to obtain records they were entitled to under Section 609(e): in some instances, customer service agents allegedly would not release records about a fraudulent account unless the victim could first name the identity thief—information available only in the very records being withheld. One victim reportedly guessed more than 30 names before giving up. The FTC also alleged that Amazon refused records to authorized law enforcement absent a subpoena and missed the FCRA’s 30-day deadline in numerous instances.

Compliance Lessons

What makes this settlement instructive is that Amazon’s alleged day-to-day practices, which included identity-verification scripts, escalation protocols, and well-intentioned “fraud prevention” efforts, did not meet the letter of the FCRA. Even after the FTC identified the issue to Amazon’s counsel in 2023, the FTC contends that the company did not implement a required written policy until 2025, after learning it was under investigation.

The parties’ resolution underscores the stakes. Amazon agreed to a $2.25 million civil penalty, detailed injunctive relief, multi-year website-notice requirements, affirmative outreach to “Eligible

Identity Theft Victims," and a decade of compliance reporting and recordkeeping. The order sunsets in 10 years.

Sophisticated Guidance Matters

The Amazon settlement illustrates that even well-intentioned compliance efforts can falter when they fail to account for the FCRA's highly specific requirements. The statute imposes precise obligations, measured in days, triggered by specific requests, and subject to carefully delineated exceptions. These obligations intersect with other regulatory regimes, such as the Gramm-Leach-Bliley Act and state law.

Businesses that touch consumer data, payments, fraud response, or identity verification need experienced counsel who understand both the letter of the FCRA and how the Commission develops and resolves these cases.