ALSTON & BIRD

WWW.ALSTON.COM

Privacy & Data Security ADVISORY ■

JUNE 23, 2020

FTC Expands Its FCRA Enforcement Activity in Action Against Retailer

***by* Kathleen Benway *and* Jon Knight**

Most businesses are already familiar with the Fair Credit Reporting Act (FCRA) and the various requirements to protect the fairness, accuracy, and privacy of consumer credit information. However, a recent Federal Trade Commission (FTC) enforcement action against retailer Kohl's Department Store Inc. has brought a rarely used provision of the statute to light.

This provision—codified at 15 U.S.C. § 1681g(e)—requires businesses to provide, upon request, certain records about commercial transactions to potential victims of identity theft. The FTC's complaint against Kohl's is the first time it has alleged a violation of this provision. Risk professionals and businesses should take notice whenever the FTC announces new areas of enforcement, as it could signal greater scrutiny by the agency. This case is no exception.

Relevant Provisions of Section 1681g(e)

The Fair and Accurate Credit Transactions Act (FACTA), which amended the FCRA in December 2003, was intended to enhance consumer protections, especially for identity theft. The most well-known provision of FACTA provides consumers with free access to their credit reports annually. FACTA also added Section 1681g(e), which requires that if a business has provided credit to or entered into a commercial transaction with a person who has allegedly committed identity theft, then the business must provide a copy of application and business transaction records upon request to the victim of the alleged identity theft or any law enforcement agency or office authorized by the victim to receive the records, no later than 30 days after the date of receipt of a request from a victim. In other words, when a consumer spots unauthorized charges or lines of credit and requests copies of records to establish the charges are not theirs, the business must comply.

There are, however, two exceptions. First, the statute does not require businesses to "obtain, retain, or maintain information or records that are not otherwise required to be obtained, retained, or maintained in the ordinary course of its business or under other applicable law." Second, the business is not required to provide "Internet navigational data or similar information about a person's visit to a website or online service."

Before providing the requested records, the business must both verify the identity of the victim and receive evidence that a claim of identity theft has been made, using the criteria the statute sets forth. The statute also specifies how a victim must make their request (in writing and mailed to an address set by the business) and that the information required by the statute must be provided without charge to the victim.

Kohl's Alleged Violations of Section 1681g(e)

According to the FTC's complaint filed in the Eastern District of Wisconsin on June 8, 2020, Kohl's internal policies between February 2017 and April 2019 prohibited giving the required statutory records directly to identity theft victims. Before February 2017 and again after April 2019, Kohl's policy for complying with victims' requests provided for victims to receive records in accordance with the statute. But beginning in February 2017, for Internet-based orders, Kohl's would only share information with law enforcement or with a victim's attorney. Kohl's later decided it would give certain customers limited information such as statements, receipts, and applications, but would only provide other required records, such as the addresses and phone numbers listed on a fraudulent application or the shipping address used for fraudulent orders, directly to law enforcement. In other words, even though the statute refers to requests from "victims," the only requests Kohl's would recognize were those from law enforcement. The FTC alleged these policies were clear violations of Section 1681g(e)'s requirements to provide records and to do so within 30 days of a request. The complaint further alleged that Kohl's actions also constituted unfair or deceptive acts or practices in violation of Section 5(a) of the FTC Act.

The Settlement

The court entered a stipulated order settling the complaint on June 10, 2020. The order includes a permanent injunction against violating Section 1681g(e), civil penalties of $220,000 for violating the FCRA, a requirement that Kohl's provide notice of the settlement to potential victims, and a requirement that Kohl's establish an extensive compliance program for Section 1681g(e) requests. The notice provisions require Kohl's to establish a website within 30 days informing potential victims of their rights under the law. It also gives Kohl's just 14 days to either provide the requested records to all victims who previously made requests or to notify those victims that Kohl's would provide the requested records upon receipt of identity verification information.

The Kohl's Settlement Highlights Key Considerations for Businesses

Is Section 1681g(e) limited to credit reporting agencies?

No. The provision here applies to any business that has "provided credit to, provided for consideration products, goods, or services to, accepted payment from, or otherwise entered into a commercial transaction for consideration with, a person who has allegedly made unauthorized use of the means of identification of the victim." In other words, if your business engages in a commercial transaction with someone who has used the identification or financial information of another without their authority, then the law will likely apply to you.

How likely is the FTC to bring similar enforcement actions in the future?

Obviously, the Kohl's case is a sample size of one and should not necessarily be seen as a trend toward greater FTC enforcement in this area. However, the FTC will view the Kohl's case as providing notice to other

businesses about the need to comply with Section 1681g(e). This means that in any future enforcement actions, the FTC may seek more onerous relief, including higher civil penalties.

Is my business even aware of the requirement to provide information to potential victims of identity fraud?

Given the lack of prior enforcement, it is possible that risk professionals have not considered whether their business has addressed the requirements of Section 1681g(e). The Kohl's case is a great opportunity to confirm that your business has a method for potential identity theft victims to make requests for their relevant records. Additionally, you should confirm that you have a basic process and standards in place for confirming the identity of potential victims and providing them with the requested information, all within the 30-day deadline set by law.

What sort of records should my business keep to reduce the likelihood of FTC inquiry or investigation?

While it may be impossible to prevent the FTC from making an inquiry, having easily accessible and organized records showing your business complies with Section 1681g(e) will go a long way toward short-circuiting a full FTC investigation. The Kohl's order helpfully lays out a roadmap for the types of records the FTC would want to see. Consider retaining records showing:

- All written consumer complaints relating to requests for records under Section 1681g(e), as well as any response.
- Each request for records covered by Section 1681g(e), including the date you received each request and the type of information the victim provided to verify their identity.
- The information you provided, if anything, in response to the request and the timing of the response.
- The reasons for any denial of a request under Section 1681g(e).

My business collects information that is protected from disclosure to third parties under a variety of state and federal privacy statutes. Am I liable under these statutes if I disclose identifying information to a victim under Section 1681g and later discover that there was no underlying identity theft?

Likely no. Section 1681g specifically provides that a business entity may not be held civilly liable under any provision of federal, state, or other law for disclosure made in "good faith." While the statute does not define what constitutes good faith, it does lays out how to confirm there is an underlying claim of identity theft: (1) receiving "a copy of a police report evidencing the claim of the victim of identity theft"; or (2) receiving an affidavit. Making disclosures only when these statutory requirements are satisfied will likely be seen as a strong indicator of good faith.

Must my business always provide information whenever we receive a request from a victim?

No. The statute allows businesses decline to provide information after making a good-faith determination that: (1) the law does not require disclosure of the information; (2) the business does not have a "high degree of confidence in knowing the true identity of the individual requesting the information"; or (3) the request is "based on a misrepresentation of fact by the individual requesting the information relevant to the request for information."

You can subscribe to future ***Privacy & Data Security*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kelley Connolly Barnaby
202.239.3687
kelley.barnaby@alston.com

Kathleen Benway
202.239.3034
kathleen.benway@alston.com

Chris Baugher
404.881.7261
chris.baugher@alston.com

Alexander G. Brown
404.881.7943
alex.brown@alston.com

Elizabeth Broadway Brown
404.881.4688
liz.brown@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

David Carpenter
404.881.7881
david.carpenter@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Kimberly K. Chemerinsky
213.576.1079
kim.chemerinsky@alston.com

Helen Christakos
650.838.2091
helen.christakos@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Maki DePalo
404.881.4280
maki.depalo@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

Stephanie A. Jones
213.576.1136
stephanie.jones@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Amy Mushahwar
202.239.3791
amy.mushahwar@alston.com

Wim Nauwelaerts
+32.2.550.3709
202.239.3709
wim.nauwelaerts@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Cara M. Peterman
404.881.7176
cara.peterman@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Jessica C. Smith
213.576.1062
jessica.smith@alston.com

Lawrence R. Sommerfeld
404.881.7455
larry.sommerfeld@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Richard R. Willis
+32.2.550.3700
richard.willis@alston.com

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ALSTON & BIRD

WWW.ALSTON.COM