DREHER TOMKIES LLP

ALERT

FOR CLIENTS AND FRIENDS OF DREHER TOMKIES LLP

March 23, 2020

OCC ISSUES SUPPLEMENTAL FAQS ON THIRD-PARTY RISK MANAGEMENT; ADDRESSES DATA AGGREGATION

Earlier this month, the Office of the Comptroller of the Currency ("OCC") released OCC Bulletin 2020-10, which sets forth frequently asked questions ("FAQs") on regulated banks' third-party risk management responsibilities. The new FAQs are intended to supplement the OCC's 2013 third-party relationship risk management guidance and clarify the OCC's expectations as banks' business arrangements become more varied and complex. The new FAQs incorporate unchanged FAQs from OCC Bulletin 2017-21 (except for one minor change) and rescind the 2017 bulletin.

Of note, the FAQs provide guidance on when a data aggregator forms a third party relationship with a bank in connection with collecting customer-permissioned data from a bank and becomes subject to a bank's third-party risk management program. In a circular response, the OCC stated that a bank has a third-party relationship when it has a business arrangement with the data aggregator. As explained by the OCC, the term "business arrangement" is meant to be broad and is synonymous with the term third party relationship.

The OCC provided two helpful examples of when a bank has a third-party relationship with a data aggregator: (1) a bank contracts or partners with a data aggregator to use data aggregation services to offer or enhance the bank's products or services and (2) a bank has a contractual relationship with a data aggregator to share customer-permissioned data, such as through an API. The key focus of a bank's third-party risk management of data aggregators should be information security and safeguarding sensitive customer data. The OCC acknowledged that when a bank is not receiving a direct service or benefit from a data aggregator, the bank has less risk. Nonetheless, the OCC expects a bank to undertake some due diligence of a data aggregator to gain assurance that a data aggregator maintains controls for safeguarding sensitive bank customer data.

Conversely, the OCC determined that typical screen scraping activities do not involve a third party relationship between the bank and a data aggregator. The OCC expects banks to take appropriate actions to manage the risks of sharing customer-permissioned data with third parties through screen scraping. According to the OCC, banks should identify large-scale screen scraping activities and take appropriate steps to learn more about the source of these activities and the screen scraper's controls to manage its data-sharing activities.

Other new FAQs may be of interest to banks leveraging innovation, including FAQs on (i) third-party risk management expectations when a bank obtains alternative data from a third party, (ii) third-party risk management when using a third-party model or a third party to help validate a third-party model, (iii) third-party risk management expectations with cloud computing services and (iv) a bank's due diligence and ongoing monitoring responsibilities when a third party does not have the ability to provide the same level of due diligence-related information as a larger institution. In addition, the new FAQs address general third-party risk management questions, such as what process a bank's board of directors must go through to approve contracts with third parties involved in "critical activities."

A bank's third-party risk management responsibilities often can create challenges for nonbanks looking to partner or that partner with banks. Banks are subject to a burdensome regulatory scheme that can seem foreign to companies without experience in the banking space. While third-party risk management responsibilities can be cited by banks to support a requirement or restriction it wants to impose on a third party relationship, third-party risk management responsibilities are set by prudential regulators. Whether or not (i) the OCC's determination that certain data aggregators have third party relationships with banks and (ii) the OCC's expectation that a bank take appropriate risk management actions with respect to screen scraping, will cause banks to restrict third-party access to customer-permissioned data remains to be seen. ❑

✧ *Mike Tomkies and Susan Seaman*

Darrell L. Dreher
ddreher@dltlaw.com

Elizabeth L. Anstaett
eanstaett@dltlaw.com

Emily C. Cellier
ecellier@dltlaw.com

Susan L. Ostrander
sostrander@dltlaw.com

2750 HUNTINGTON CENTER
41 S. HIGH STREET
COLUMBUS, OHIO 43215
TELEPHONE: (614) 628-8000 FACSIMILE: (614) 628-1600
WWW.DLTLAW.COM

Michael C. Tomkies
mtomkies@dltlaw.com

Susan M. Seaman
sseaman@dltlaw.com

Lindsay P. Valentine
lvalentine@dltlaw.com

Judith M. Scheiderer
jscheiderer@dltlaw.com

Robin R. De Leo
robin@deher-la.com