

OFAC RISK ISN'T VIRTUAL FOR DIGITAL CURRENCY PAYMENT PROCESSORS

On February 18, 2021, the US Department of the Treasury's Office of Foreign Assets Control ("OFAC") announced a settlement of apparent US sanctions violations by Atlanta, Georgia-based BitPay, Inc. ("BitPay") involving its provision of digital currency payment processing services to purchasers of goods and services located in Crimea, Cuba, Iran, North Korea, Sudan and Syria.¹

The case highlights the sanctions risks for US companies that provide services in connection with digital currency payments and indicates sanctions compliance controls that may be appropriate to mitigate such risks. BitPay did not voluntarily self-disclose the apparent violations, but OFAC determined that they were not egregious and therefore assessed a base penalty of \$2,255,000. OFAC then reduced the final penalty to \$507,375 based on a number of mitigating factors including BitPay's cooperation with OFAC, remedial measures and compliance enhancements.

During June 2013 to September 2018, BitPay processed 2,102 transactions on behalf of individuals located in OFAC-sanctioned jurisdictions who were purchasing goods or services from merchants using BitPay's digital currency payment processing services. BitPay received digital currency payments from the individuals located in sanctioned jurisdictions, converted the digital currency into fiat currency, and then relayed the payments to its merchant customers. OFAC determined that although BitPay screened its merchant customers against the OFAC Specially Designated Nationals (SDN) list and conducted due diligence to confirm that the merchants were not located in sanctioned jurisdictions, that it failed to screen data of the individual buyers that it received. Specifically, BitPay received information at the time of certain transactions that included the individual buyers' names, addresses, emails, and phone number that indicated the buyers were located in sanctioned jurisdictions. Further, from November 2017 onwards, BitPay obtained buyers' IP addresses. However, OFAC determined that BitPay's transaction review process failed to analyze this data for sanctions compliance purposes. OFAC found that BitPay "failed to exercise due caution or care for its

¹ See https://home.treasury.gov/system/files/126/20210218_bp.pdf

sanctions compliance obligations when it allowed persons in sanctioned jurisdictions to transact with BitPay's merchants using digital currency for approximately five years, even though BitPay had sufficient information to screen those customers."

After learning of the OFAC violations, BitPay adopted remedial measures that included: (i) implementing mechanisms to block buyers with IP addresses in sanctioned jurisdictions from connecting to the BitPay website or viewing instructions on how to make a payment; (ii) conducting sanctions reviews of buyers' physical and email addresses when provided by merchants; and (iii) launching a mandatory identification tool for buyers wishing to make a digital currency payment equivalent to \$3,000 or more, which requires buyers to provide an email address, proof of identification/photo ID, and a selfie photo.

Previous OFAC settlements also have identified that companies providing online services, including financial institutions providing online account services, should use IP blocking mechanisms and screening to mitigate sanctions risks.² Companies providing digital currency services also should review OFAC's FAQs on virtual currency that among other things emphasize that "firms that facilitate or engage in online commerce or process transactions using digital currency, are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade or investment-related transactions."³

² For example, see our [briefing](#) on OFAC's December 2020 settlement with BitGo, Inc.

³ See <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626>.

CONTACTS

David DiBari
Managing Partner
T +1 202 912 5098
E david.dibari
@cliffordchance.com

Steven Gatti
Partner
T +1 202 912 5095
E steven.gatti
@cliffordchance.com

Megan Gordon
Partner
T +1 202 912 5021
E megan.gordon
@cliffordchance.com

George Kleinfeld
Partner
T +1 202 912 5126
E george.kleinfeld
@cliffordchance.com

Celeste Koeleveld
Partner
T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Michelle Williams
Partner
T +1 202 912 5011
E michelle.williams
@cliffordchance.com

Philip Angeloff
Counsel
T +1 202 912 5111
E philip.angeloff
@cliffordchance.com

Jacqueline Landells
Counsel
T +1 202 912 5061
E jacqueline.landells
@cliffordchance.com

Robert Rice
Counsel
T +1 212 878 8529
E robert.rice
@cliffordchance.com

David Adams
Associate
T +1 202 912 5067
E davidg.adams
@cliffordchance.com

Jesse Overall
Associate
T +1 212 878 8289
E jesse.overall
@cliffordchance.com

John-Patrick Powers
Associate
T +1 202 912 5048
E john-patrick.powers
@cliffordchance.com

Holly Bauer
Associate
T +1 202 912 5132
E holly.bauer
@cliffordchance.com

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

© Clifford Chance 2020

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.