Volume 4, No. 4 | July–August 2021

RAIL

The Journal of Robotics, Artificial Intelligence & Law

Editor's Note: AI Developments
Steven A. Meyerowitz

National Security Commission on Artificial Intelligence Final Report Prioritizes U.S. Global Competition, Conflict Preparation, and Enhanced Protection of Privacy and Civil Liberties
Katherine Sheriff and K.C. Halm

Advancing America's Dominance in AI: The 2021 National Defense Authorization Act's AI Developments
Jonathan M. Baker, Adelicia R. Cliffe, Kate M. Growley, Laura J. Mitchell Baker, and Michelle D. Coleman

FDA Releases Action Plan for Artificial Intelligence/Machine Learning-Enabled Software as a Medical Device
Nathan A. Brown, Christin Helms Carey, and Emily I. Gerry

Deepfake Litigation Risks: The Collision of AI's Machine Learning and Manipulation
Erin M. Bosman, Christine E. Lyon, Michael Burshteyn, and Benjamin S. Kagel

FBI Warns Companies of "Almost Certain" Threats from Deepfakes
Matthew F. Ferraro, Jason C. Chipman, and Benjamin A. Powell

Prepare for the Impending Wave of Facial Recognition Technology Regulation—Before It's Too Late
David J. Oberly

Considerations in Machine Learning-Led Programmatic Underwriting
Scott T. Lashway, Christopher A. Lisy, and Matthew M.K. Stein

Making Safer Robotic Devices
William D. Kennedy, James D. Burger, and Frank A. Bruno

OFAC Settles With Digital Currency Services Provider for Apparent Violations of Multiple Sanctions Programs
Gustavo J. Membiela and Natalia San Juan

Report on ExamSoft's ExamID Feature (and a Method to Bypass It)
Gabe Teninbaum

Current Developments: AI Research, Crypto Cases Make News
Victoria Prussen Spears

Everything Is Not *Terminator*: The AI Genie Bottle
John Frank Weaver

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 4, No. 4 | July–August 2021

239 **Editor's Note: AI Developments**
Steven A. Meyerowitz

243 **National Security Commission on Artificial Intelligence Final Report Prioritizes U.S. Global Competition, Conflict Preparation, and Enhanced Protection of Privacy and Civil Liberties**
Katherine Sheriff and K.C. Halm

251 **Advancing America's Dominance in AI: The 2021 National Defense Authorization Act's AI Developments**
Jonathan M. Baker, Adelicia R. Cliffe, Kate M. Growley, Laura J. Mitchell Baker, and Michelle D. Coleman

255 **FDA Releases Action Plan for Artificial Intelligence/Machine Learning–Enabled Software as a Medical Device**
Nathan A. Brown, Christin Helms Carey, and Emily I. Gerry

261 **Deepfake Litigation Risks: The Collision of AI's Machine Learning and Manipulation**
Erin M. Bosman, Christine E. Lyon, Michael Burshteyn, and Benjamin S. Kagel

267 **FBI Warns Companies of "Almost Certain" Threats from Deepfakes**
Matthew F. Ferraro, Jason C. Chipman, and Benjamin A. Powell

271 **Prepare for the Impending Wave of Facial Recognition Technology Regulation—Before It's Too Late**
David J. Oberly

277 **Considerations in Machine Learning-Led Programmatic Underwriting**
Scott T. Lashway, Christopher A. Lisy, and Matthew M.K. Stein

283 **Making Safer Robotic Devices**
William D. Kennedy, James D. Burger, and Frank A. Bruno

289 **OFAC Settles With Digital Currency Services Provider for Apparent Violations of Multiple Sanctions Programs**
Gustavo J. Membiela and Natalia San Juan

293 **Report on ExamSoft's ExamID Feature (and a Method to Bypass It)**
Gabe Teninbaum

301 **Current Developments: AI Research, Crypto Cases Make News**
Victoria Prussen Spears

311 **Everything Is Not *Terminator*: The AI Genie Bottle**
John Frank Weaver

EDITOR-IN-CHIEF

Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Miranda Cole
Partner, Covington & Burling LLP

Kathryn DeBord
Partner & Chief Innovation Officer, Bryan Cave LLP

Melody Drummond Hansen
Partner, O'Melveny & Myers LLP

Paul B. Keller
Partner, Allen & Overy LLP

Garry G. Mathiason
Shareholder, Littler Mendelson P.C.

Elaine D. Solomon
Partner, Blank Rome LLP

Linda J. Thayer
Partner, Finnegan, Henderson, Farabow, Garrett & Dunner LLP

Edward J. Walters
Chief Executive Officer, Fastcase Inc.

John Frank Weaver
Attorney, McLane Middleton, Professional Association

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2021 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2021 Full Court Press, an imprint of Fastcase, Inc.

All Rights Reserved.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

OFAC Settles With Digital Currency Services Provider for Apparent Violations of Multiple Sanctions Programs

Gustavo J. Membiela and Natalia San Juan*

The U.S. Department of the Treasury's Office of Foreign Assets Control published an enforcement action discussing a recent settlement with BitPay Inc., whose platform facilitates merchants' acceptance of digital currency as payment for goods and services, to resolve 2,102 apparent violations of multiple U.S. sanctions programs. The authors of this article discuss the settlement and the five essential components of compliance.

What Happened?

The U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") settled with BitPay Inc. for $507,375 to resolve 2,102 apparent violations of multiple U.S. sanctions programs for allowing individuals located in sanctioned jurisdictions to use digital currency on its platform to transact with merchants in the United States and elsewhere.

The Bottom Line

This was the second OFAC enforcement action against a digital currency services provider published in a two-month period. Companies providing digital currency services, like all financial service providers, should be aware of sanctions risks associated with providing such services. This action emphasizes the importance of developing and implementing tailored, risk-based sanctions compliance procedures sufficient to ensure that companies do not deal with blocked persons or engage in transactions prohibited by U.S. sanctions.

Robotics, Artificial Intelligence & Law / July–August 2021, Vol. 4, No. 4, pp. 289–292.
© 2021 Full Court Press. All rights reserved.
ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

The Story

On February 18, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control published an enforcement action discussing a recent settlement with BitPay Inc., a company based in Atlanta, Georgia, whose platform facilitates merchants' acceptance of digital currency as payment for goods and services. That is, BitPay receives digital currency on behalf of its merchants, converts the digital currency to fiat currency, and then transmits that currency to its merchants. BitPay settled for $507,375 after the company faced, at a maximum, a $619,689,816 civil monetary penalty for 2,102 apparent violations of multiple U.S. sanctions programs.

From approximately June 10, 2013, to September 16, 2018, BitPay processed 2,102 digital currency transactions on behalf of buyers located in sanctioned jurisdictions, including Cuba, Crimea, Iran, North Korea, Sudan, and Syria. OFAC noted that, at the time of the apparent violations, BitPay screened its direct customers, the merchants, and conducted due diligence to ensure they were not located in sanctioned jurisdictions. BitPay also obtained the location information, including Internet Protocol ("IP") addresses, from its merchants' buyers, but it failed to use that location information to screen the buyers for sanctions compliance purposes. As a result, individuals in sanctioned jurisdictions were able to make purchases from merchants in the United States and elsewhere.

To calculate the final settlement amount, OFAC listed two aggravating factors against BitPay.

First, for approximately five years, the company failed to exercise due caution by not preventing buyers located in sanctioned jurisdictions from transacting with BitPay's merchants using digital currency. OFAC emphasized that BitPay could have screened the location data it obtained about its merchants' buyers to ensure they were not located in sanctioned jurisdictions, but the company failed to do so.

Second, BitPay's sanctions compliance deficiencies granted approximately $129,000 in economic benefit to individuals located in sanctioned jurisdictions, undermining the integrity of the sanctions programs.

On the other hand, OFAC credited six mitigating factors in favor of BitPay.

First, BitPay implemented sanctions compliance controls, such as conducting due diligence on merchant customers, as early as 2013. It also formalized its sanctions compliance program in 2014.

Second, in its training for all employees, BitPay made clear that it prohibited merchants located in sanctioned jurisdictions from signing up for its services, as well as trade with sanctioned individuals.

Third, BitPay is a relatively small company that has not received a penalty notice or Finding of Violation from OFAC in the five years preceding the first apparent violation.

Fourth, although the company did not voluntarily self-disclose, it cooperated with OFAC's investigation.

Fifth, the company has undertaken measures to minimize the risk of recurrence of the conduct that led to the apparent violations. These measures include: (1) blocking IP addresses that appear to originate in sanctioned jurisdictions, (2) checking the physical and email addresses of merchants' buyers to prevent completion of an invoice from the merchant if the individual is located in a sanctioned jurisdiction, and (3) launching a new customer identification tool for buyers paying invoices of $3,000 or more. The new merchant customer identification tool requires customers to provide an email address, proof of identification, and a selfie photo.

Lastly, as part of the settlement, the company has agreed to continue the implementation of these and other compliance commitments.

This was the second OFAC enforcement action to target a digital currency services provider in less than two months, demonstrating OFAC's increased enforcement attention on digital currencies. On December 30, 2020, OFAC announced its settlement with BitGo Inc., a California-based technology company that facilitates digital currency transactions and provides non-custodial digital wallet management services. In that case, OFAC settled with BitGo for $98,830, resolving 183 apparent violations of multiple U.S. sanctions programs for processing digital currency transactions on behalf of individuals located in sanctioned jurisdictions. As in the case of BitPay, OFAC noted that, at the time of the apparent violations, BitGo tracked its users' IP addresses for security and login purposes, but did not use their IP addresses to screen users for sanctions compliance.

Conclusion

OFAC's recent enforcement actions caution persons subject to U.S. jurisdiction of the sanctions' risks associated with the provision of digital currency services. They demonstrate the need for companies to maintain tailored, risk-based sanctions compliance procedures and internal controls to ensure that they do not engage in unauthorized transactions prohibited by U.S. sanctions.

Although there is no single compliance program or solution suitable for every circumstance, the enforcement actions emphasize that OFAC expects companies to implement at least five essential components of compliance outlined in OFAC's *A Framework for OFAC Compliance Commitments*:

(1) Management commitment;
(2) Risk assessment;
(3) Internal controls;
(4) Testing and auditing; and
(5) Training.

Administrators, exchangers, and other companies engaged in digital currency services should exercise caution to prevent persons located in sanctioned jurisdictions from using their services by, for example, screening all available information, to mitigate sanctions risks. Such companies can benefit from developing and maintaining a compliance-first culture with proper risk assessments, internal controls, testing and auditing, and employee training.

Note

* Gustavo J. Membiela is a partner at Hunton Andrews Kurth, focusing his practice on commercial litigation and cross-border disputes, including arbitration and investigations. Natalia San Juan is an associate on the firm's litigation team, focusing on commercial litigation and arbitrations. The authors may be reached at gmembiela@huntonak.com and nsanjuan@huntonak.com, respectively.