Fair Warnings from OFAC’s Settlements with Cryptocurrency Service Providers: Compliance Should Include Lifetime-of-the-Relationship, In-Process Geolocational Checks

Sarah Jane Hughes  
*Indiana University Maurer School of Law, sjhughes@indiana.edu*

Follow this and additional works at: [https://www.repository.law.indiana.edu/facpub](https://www.repository.law.indiana.edu/facpub)

Part of the Banking and Finance Law Commons, Commercial Law Commons, Internet Law Commons, and the Law and Economics Commons

**Recommended Citation**

Hughes, Sarah Jane, "Fair Warnings from OFAC’s Settlements with Cryptocurrency Service Providers: Compliance Should Include Lifetime-of-the-Relationship, In-Process Geolocational Checks" (2023). *Articles by Maurer Faculty*. 3073.  
[https://www.repository.law.indiana.edu/facpub/3073](https://www.repository.law.indiana.edu/facpub/3073)

This Article is brought to you for free and open access by the Faculty Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Articles by Maurer Faculty by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact kdcogswe@indiana.edu.
Internet Law & Cyber-Security
(Hits://Businesslawtoday.Org/Practice-Area/Internet-Law-Cyber-
Security/) 
Business Regulation & Regulated Industries
(Hits://Businesslawtoday.Org/Practice-Area/Business-Regulation-
Regulated-Industries/)

Fair Warnings from OFAC’s Settlements with Cryptocurrency Service Providers: Compliance Should Include Lifetime-of-the-Relationship, In-Process
Geolocational Checks

By: Sarah Jane Hughes (/author/sarah-jane-hughes/)
| February 21, 2023

In 2022, the Office of Foreign Assets Control (OFAC) announced numerous settlements with cryptocurrency exchanges. These settlements serve as “fair warnings” to all cryptocurrency service providers who are “U.S. persons” or who offer services to U.S. persons. The term “U.S. persons” is defined in 31 C.F.R. §560.314 as “any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.”

This article focuses on these “fair warnings” as they have accumulated from prior settlements and from OFAC’s published guidance on compliance requirements that have been public for some time.

This article uses two late 2022 OFAC settlement announcements—with West-Coast-based Bittrex, Inc. and Payward, Inc. d/b/a Kraken—to make clear that OFAC was adhering to a previously announced requirement on providers of financial services. Specifically, OFAC requires more than verification of identity at onboarding and periodic checking of customers against OFAC’s Specially Designated Nationals (SDN) list. Additionally, providers should employ lifetime-of-the-transaction and in-process geolocation checking in their interdiction screening. Geolocation screening in lifetime-of-the-relationship and in-process transactions raised the stakes for providers to block or reject transactions that would violate the sanctions regimes OFAC enforces.
The last part of this article walks through other fair warnings provided by settlements agreed to since March 2015 or other public guidance. Before discussing the two late 2022 settlements or the fair warnings, it may help to have the foundation of the March 2015 settlement OFAC made with PayPal, Inc.

**A. OFAC’S EARLY FORAY INTO IN-PROCESS TRANSACTIONS IN NEWER ELECTRONIC PAYMENTS AND SERVICES: PAYPAL, INC. (MARCH 2015)**

OFAC claimed new territory when it announced its settlement with PayPal, Inc. on March 25, 2015.[1] OFAC maintained that PayPal “did not screen in-process transactions in order to block or reject prohibited transactions.” The settlement highlighted, among other things, two types of deficiencies in PayPal’s sanctions compliance program. In the first, PayPal’s automatic interdiction filter failed to identify at least one customer as a potential SDN when OFAC made the SDN designation because its automatic interdiction filter was not “working properly.” PayPal’s agents “dismissed” on at least five occasions one customer’s SDN match and proceeded with transactions. On one other occasion, the filter “flagged” this customer’s account, but a PayPal agent again dismissed the match despite receiving additional information that showed a date of birth and place of birth identical to the SDN. These failures resulted in 136 transactions with a single individual on the SDN list that violated the “Weapons of Mass Destruction Proliferators Sanctions Regulations.”[2] The March 2015 settlement also addressed violations by PayPal of other U.S. sanctions regulations, and PayPal agreed to pay civil penalties totaling $7,658,300.[3]
1. Bittrex, Inc.

Bittrex, Inc. is a private company based in Bellevue, Washington. Bittrex provides both virtual-currency-exchange and hosted-wallet services. OFAC’s settlement announcement explained that from March 2014 to December 31, 2017, Bittrex operated more than 1,700 accounts, processed 116,421 virtual-currency-related transactions, and transacted $263,451,600.13 in violation of law and OFAC regulations.

Bittrex apparently showed “some understanding” of OFAC regulations by August 2015, months after OFAC settled with PayPal. However, until October 2017, Bittrex had no internal controls to screen customers or transactions for connections to sanctioned jurisdictions. OFAC described other failings in Bittrex’s compliance efforts, including:

- not screening IP address or physical address information that customers were in sanctioned jurisdictions;
- not paying attention to customers providing Iranian passports or identifying themselves as being in Iran at account opening;
- not scrutinizing customers or transactions for nexus to sanctioned jurisdictions; and
- failing to have any sanctions compliance program from March 2014 to February 2016. Ouch!

OFAC cited the absence of any sanctions compliance program for two years as one of three aggravating factors in determining the civil monetary penalty of more than $24 million. Among the penalty-mitigating factors was the “swiftness” with which Bittrex responded to OFAC’s Apparent Violations notice.

2. Kraken

On November 28, 2022, OFAC announced a settlement with Kraken for violations of the Iranian Transactions and Sanctions Regulation. Kraken’s parent, Payward, Inc., is
Based in San Francisco.

Based on IP address data, Kraken continued to deal with customers who had opened accounts outside of sanctioned jurisdictions and subsequently transacted business with Kraken from Iran, a sanctioned jurisdiction. The violations occurred between October 14, 2015, and June 29, 2019. Kraken's violations began six months after the PayPal settlement was announced.

OFAC cited Kraken's failure to employ geolocational in-process and after-onboarding screening as an “aggravating factor” in its penalty calculations. OFAC had concluded that Kraken had “reason to know based on available IP addresses that transactions appear to be” emanating from Iran. Ouch.

The settlement confirms that it is not sufficient to screen customers at onboarding or account opening or to perform daily checks to identify new entries on OFAC's SDN list. Because customers may transact from sanctioned jurisdictions after establishment of accounts, daily monitoring needs to track IP addresses that are the source of transaction requests and instructions to identify transactions coming from jurisdictions that are on the sanctioned lists.

In the settlement, Kraken also agreed to implement more analytical tools such as “multiple blockchain analytics tools” (MBAT). These tools are geolocation controls including Internet Protocol (IP) address-blocking systems. MBAT may be a term or service not familiar to everyone. Prominent providers of MBAT include brand-name commercial providers such as Chainalysis and CipherTrace. MBAT tools assist with the basic identification and nationality verification requirements OFAC has implemented. Kraken has agreed to do more, including screening for OFAC’s “50 Percent Rule,” which requires detailed reports on beneficial ownership of assets and blocking of clients' access to accounts and assets.
C. FAIR WARNINGS SPECIFICALLY RELATED TO CRYPTO ENTITIES’ COMPLIANCE PROGRAMS

OFAC’s settlements with Bittrex and Kraken are examples of enforcement actions presaged by prior enforcement actions and other OFAC guidance. These actions might still be cited as “regulation by enforcement“ to the extent that prior enforcement actions frame the standards being enforced against each company. For example, OFAC made its focus on newer financial products and services clear beginning with its enforcement action against PayPal, Inc. in March 2015. These issues and statements of regulatory approach are described in section A of this article.

Since PayPal’s March 2015 settlement, managers updating and maintaining suitable interdiction-filtering procedures and programs had further fair warnings of OFAC’s approach and should have implemented screening of clients who may move to sanctioned jurisdictions, or who may be sanctioned by OFAC after accounts are opened. Kraken’s transactions mentioned in the settlement announcement all came later than OFAC’s action against PayPal, Inc.

The Bittrex and Kraken settlements provide at least five specific “fair warnings“ about sufficient sanctions controls programs’ components, including warnings about (1) geolocation/IP address tools, (2) efficacy of controls, (3) being involved with facilitation of violations, (4) use of blockchain analytical tools, and (5) the totality for components of a proper sanctions compliance program. Let’s look at each.

1. *Fair warning about geolocation tools.* Kraken agreed to deploy tools such as the automated interdiction-compliance filters that commercial banks, securities firms, and insurance companies use to manage the day-to-day issues of account maintenance over the course of the provider’s relationship with its customers. For Kraken, this meant adding geolocation in-process transaction screening.
2. *Fair warning about efficacy of controls.* In addition to settlement announcements, OFAC has issued its 2021 “Sanctions Compliance Guidance for the Virtual Currency Industry” (2021 Guidance). OFAC mentions two actions, both involving money laundering and one of which involved “facilitating” Russian ransomware actors. OFAC urged the virtual currency industry to “implement effective sanctions compliance controls to mitigate the risk of sanctioned persons and other actors exploiting virtual currencies to undermine U.S. foreign policy interests and national security.”

3. *Fair warning about facilitation of violations.* The OFAC 2021 Guidance also reminded actors that “for some sanctions programs, U.S. persons, wherever located, ... are prohibited from facilitating actions on behalf of non-U.S. persons if the activity would be prohibited by sanctions regulations if directly performed by a U.S. person or within the United States.”

Virtual currency compliance programs, OFAC advised, should include “sanctions list and geographic screening,” among other measures. Details on “internal controls” in the 2021 Guidance include providers making more active use of users’ IP addresses. Additional details suggest controls via IP addresses that prevent persons in comprehensively sanctioned jurisdictions, such as Iran or Syria, from accessing providers’ platforms. OFAC expects that entities will “ensure [they are] utilizing all available information for sanctions compliance purposes.”

4. *Fair warning on blockchain analytic tools and ongoing screening.* The 2021 guidance document also suggests that virtual currency companies “consider conducting a historic lookback of transactional activity after OFAC lists a virtual currency address on the SDN list to identify connections to listed addresses.” Providers are encouraged to use blockchain analytic tools to identify and manage sanctions risks. OFAC also mentioned “ongoing sanctions screening and risk-based re-
screening” to account for updated customer information, changes in OFAC’s SDN lists, or changes in regulatory requirements.

In 2018, OFAC included known virtual currency addresses as identifying information for persons on its SDN list and allowed searches of those addresses using the “ID #” field in it Sanctions List FAQs 562, 563, and 594. OFAC provided more detail in its FAQs, some of which it updated in association with its 2022 press release announcing its settlement with Kraken.

5. **Fair warning about components of a functional sanctions compliance program.** OFAC also published on May 2, 2019, “A Framework for OFAC Compliance Commitments.” The Framework covers foreign entities that conduct business in or with the United States or U.S. persons or that use goods or services exported from the United States. The Framework identifies five aspects of a sanctions compliance program: management commitment, risk assessment, training, internal controls, and testing/auditing. Additionally, OFAC has published and codified “Economic Sanctions Enforcement Guidelines.”

Admittedly, some of the guidance that OFAC issued came after the violations covered by Kraken’s November 2022 settlement. Adding the Kraken settlement and OFAC’s FAQs updated at the time of the Kraken settlement to the universe of OFAC’s guidance provides important benchmarks for providers in the virtual currency industry.

**D. A GENERALLY APPLICABLE FAIR WARNING ON VOLUNTARY SELF-DISCLOSURE OF POSSIBLE VIOLATIONS**

OFAC seldom reveals how it becomes alerted to possible sanctions violations. It often is alerted by the entity itself through a procedure known as “voluntary self-disclosure.” Companies that self-disclose violations can negotiate much lower civil penalties. Self-disclosure requires robust and risk-based internal screening and policies to deter and detect
violations of sanctions regimes. The voluntary self-disclosure must reach OFAC before OFAC learns of a violation from another source, such as a bank or freight forwarder.

In the cases of Bittrex and Kraken, OFAC did not mention self-disclosures, which signals that another entity or government had alerted OFAC or its sister agency, the Financial Crimes Enforcement Network (FinCEN) of possible violations.

Accordingly, one more generic “fair warning” should be on the fair warnings list: *If you identify violations, get started on your self-disclosure promptly.* Or, to be more blunt: *fess up when you mess up!*

**E. CONCLUSION**

As the tools available to those intending to circumvent sanctions laws and their enablers improve, OFAC has expanded the range of tools it expects entities subject to OFAC’s strict liability regimes to employ. This requires U.S. person subject to OFAC’s risk-based compliance expectations to reassess their compliance tools and procedures. Although the Federal Aviation Administration may use a thirty-year-old software to run a notice to pilots before take-off, providers of financial products and services subject to OFAC’s jurisdiction should not fail to update their systems that can detect and prevent transactions with sanctioned individuals and entities or sanctioned nation-states. Finally, providers should make voluntary self-examination and self-disclosure protocols key parts of their OFAC compliance programs.

All rights reserved. © Sarah Jane Hughes 2023.

Sarah Jane Hughes is the University Scholar and Fellow in Commercial Law at the Maurer School of Law, Indiana University in Bloomington, Indiana. Before joining the faculty as a visiting professor in 1989, Ms. Hughes was an
Attorney-Advisor at the Federal Trade Commission focusing on retail payments, consumer credit protection (including the enforcement of the Truth-in-Lending Act and the FTC’s trade regulation rule Preservation of Consumers’ Claims and Defenses), and financial privacy issues. Read her full bio here (https://businesslawtoday.org/author/sarah-jane-hughes/).

1. Available at
   (about:blank). ↑

2. 31 C.F.R. §544. ↑

3. Available at
   (about:blank). ↑

4. Available at
   (about:blank). ↑

5. 31 C.F.R. § 560.204. ↑

6. Available at https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20211015
   (about:blank). ↑


10. Available at
    (about:blank). ↑


By: Sarah Jane Hughes ([author/sarah-jane-hughes/](https://home.treasury.gov/policy-issues/financial-sanctions/faqs/13)).

| February 21, 2023 |