

**DILENDORF**  
LAW FIRM

# **Coming In Hot: Crypto In Rem Seizure Forfeiture Actions**

Authors: Max Dilendorf, Esq.  
and Micaela Baldner

# Table Of Contents

Coming In Hot: Crypto In Rem Seizure Forfeiture Actions ..... 1

The Relevance of Blockchain Wallets .....2

Summary .....5

Contacts.....7

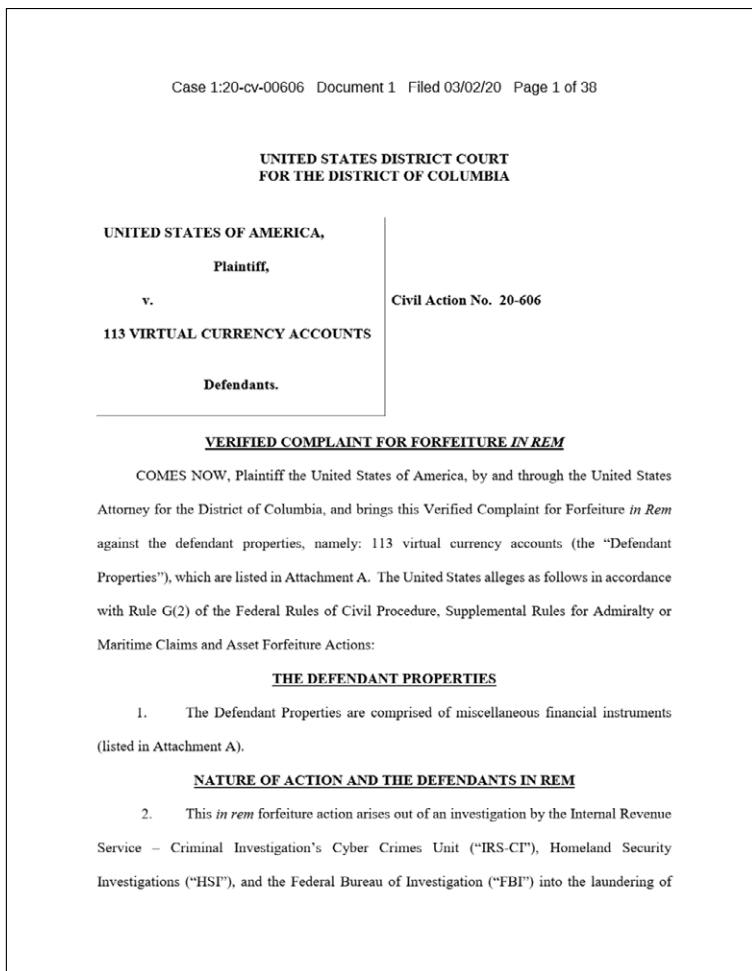
# Coming In Hot: Crypto In Rem Seizure Forfeiture Actions

It is well-established that the crypto industry has gained traction in the last several years. As such, the Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), and the Internal Revenue Service's Criminal Investigation's Cyber Crimes Unit (IRS-CI) have been hard at work to reduce the likelihood of wire fraud, money laundering, and other types of criminal transactions from taking place on blockchain platforms. For instance, to hold anonymously acting criminals accountable, the U.S. government has begun to file *in rem* civil forfeiture actions against "dirty" blockchain wallets to extinguish their use value in financial markets. This move is both unprecedented and significant as it allows the government to seize the assets in question, ultimately depriving their current possessors of the power to dispose of or profit from them. It is important to note that the U.S. government is bringing these forfeiture actions without knowing if the owners of such blockchain wallets are located in the United States. Why? Because it does not matter. The U.S. government is legally able to go after any and all individuals or entities, whether anonymously acting or not, engaged in criminal transactions that violate U.S. laws. In short, this legal move is the government's checkmate. In fact, practically speaking, *in rem* crypto forfeiture actions are not only available to the federal government, but they could also be used within the private sector in divorce settlements or partnership dispute resolutions to name a few. If you would like to learn more, take a look at two of the latest *in rem* lawsuits filed by the U.S. government against blockchain wallets.

# The Relevance of Blockchain Wallets

To understand the socioeconomic implications of the government’s successful *in rem* civil forfeiture lawsuits, it is important to first discuss the relevance of blockchain wallets within the larger cryptocurrency framework. It is well-known that the value of blockchain wallets lies in the concept of a private key, as the individual or entity that controls the private key also controls the

value associated with the corresponding public address. Consequently, the cryptographic relationship between private and public keys has led many actors within the crypto space to believe that blockchain wallets are untouchable, or rather shielded from government intervention, as such wallets can only be accessed by those who know the private key code. However, it is important for crypto investors, businesses, and the community at large to understand that the government already possesses the ability to seize digital wallets—without



*In Rem Lawsuit 1*

United States District Court  
Eastern District of Michigan  
Southern Division

United States of America,

Plaintiff,

Civil No.

vs.

Honorable:

Dell PowerEdge Server, Serial  
Number JNFHSW1, and

Any and All Cryptocurrency or  
Other Digital Assets Contained  
in Virtual Currency Wallets Residing  
on the Dell PowerEdge Server, Serial  
Number JNFHSW1,

Defendants *in rem*.

---

**Complaint for Forfeiture**

---

Now comes Plaintiff, the United States of America, by and through its undersigned attorneys, and states upon information and belief in support of this Complaint for Forfeiture as follows:

**JURISDICTION AND VENUE**

1. This is an *in rem* civil forfeiture action pursuant to 18 U.S.C. § 981(a)(1)(A), resulting from a violation or violations of 18 U.S.C. § 1960, seeking forfeiture of Defendants *in rem*.

*In Rem Lawsuit 2*

needing to first obtain the private key codes—in the same way it is able to sanction and blacklist traditional bank accounts. Thus, blockchain wallets are proving to be less untouchable than many believed or hoped them to be.

In an effort to continue the trend toward increased crypto regulation, in October of 2020, the Department of Justice (DOJ) issued its Cryptocurrency Enforcement Framework (Report). In that Report, the DOJ set out several dangers and enforcement proposals related

to crypto-related crime.<sup>1</sup> Specifically, the Report addresses how the government plans to continue to rely on digital asset forfeiture efforts to fight against criminal actors within the crypto space. For instance, the Report states that the Department already uses available civil authorities for seizures and forfeitures, which allows it to “arrest” individual assets themselves, even in cases where no person is charged criminally or where the defendant may not be prosecutable

---

<sup>1</sup> Report of the Attorney General’s Cyber Digital Task Force, U.S. Dep’t of Justice (Oct. 2020), <https://www.justice.gov/archives/ag/page/file/1326061/download>

due to death or flight from a jurisdiction.<sup>2</sup> In fact, the government has gone as far as to prosecute blockchain wallets operated by individuals or entities seeking to avoid criminal responsibility by hiding behind their anonymously crafted personas.

To do this, prosecutors begin by filing an *in rem* action. If after months of litigation a federal judge issues a default judgment against the unlawful blockchain wallets, then the government has the power to blacklist those wallets with the Financial Crimes Enforcement Network (FinCEN). At that point, FinCEN has both the ability to set an alarm on the wallets to track their movement and the authority to demand that crypto exchange platforms do not do business with them. Moreover, the Treasury's Office of Foreign Assets Control (OFAC) has a list of Specially Designated Nationals And Blocked Persons (SDN), which contains the names or addresses of blockchain wallets that are not allowed to transact or do business with any U.S.-based individuals or entities.<sup>3</sup> Accordingly, the belief that the U.S. government is far behind in cryptocurrency regulation is simply no longer accurate as the government's regulatory actions are both far reaching and have the potential to affect individuals or entities operating within and outside of American borders.<sup>4</sup>

For instance, in March of 2020, the U.S. government filed an *in rem* lawsuit against 113 virtual currency accounts in the United States District Court for the District of Columbia. In its complaint, the U.S. government argued that the North Korean government had "used cyberspace to launch increasingly sophisticated attacks to steal funds from financial institutions and cryptocurrency exchanges

---

<sup>2</sup> Id. at 21.

<sup>3</sup> Specially Designated Nationals List Update, U.S. U.S. Dep't of Treas. (Sept. 16, 2020), <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20200916>

<sup>4</sup> Id. at 25.

to generate income.”<sup>5</sup> Expressly, the complaint alleged three theories of forfeiture: (1) the virtual currencies were sent into and out of the United States in furtherance of an act of theft; (2) the virtual currencies were used as property involved in international promotional money laundering; and (3) the virtual currencies were property of North Korea, a designated state sponsor of terrorism.<sup>6</sup> This lawsuit is particularly important as the successful investigations into the North Korean money-laundering scheme demonstrate the urgency with which the U.S. government is both implementing regulatory strategies aimed at disenfranchising bad actors hiding behind anonymous blockchain wallets and actively curtailing criminal activity from occurring within the virtual currency space.

## Summary

As Olaf Carlson-Wee, Founder and CEO of Polychain Capital, recently stated in a video interview, U.S. hyper regulation at the inception of the internet would not have stopped Silicon Valley from existing, but it could have driven the minds behind those projects to establish the technological hub outside of American borders. Likewise, while crypto regulation has the ability to expand the investor base by bringing more legitimacy to the industry as a whole, regulators have to consider how far they want to go with their regulatory efforts, as hyper regulation may sway individuals, corporations, and crypto projects away from establishing roots in the United States. Within this premise, while it is clearly

---

<sup>5</sup> Complaint at 5, *United States v. 113 Virtual Currency Accts.* (D.D.C. Mar. 2, 2020) (No. CV 20-606).

<sup>6</sup> *Id.*


beneficial that the U.S. government is able to blacklist dirty blockchain wallets and provide a safer space for the rest of society to transact and economically advance, regulators must continue to grant creative minds enough flexibility to foster innovation via means of experimentation and risk-taking activities. This intentional action will signal that the U.S. government is on the side of those who produce the technologies that have the potential to revolutionize the way we interact, live, and experience the ever-changing world by pushing our modern American digital economy toward a competitive and transformative yet level playing field. At Dilendorf Law, our legal team works with top industry investigators and blockchain analytical tools to provide clients with answers to difficult questions involving the seizure of blockchain wallets and the separation of crypto assets. If you would like to learn more about our services, please contact our legal team or visit our website for more information.





### **Dilendorf Law Firm, PLLC**

 [md@dilendorf.com](mailto:md@dilendorf.com)


 +1-212-457-9797

 Dilendorf Law Firm  
4 World Trade Center Suite 2979  
New York, NY 10006

### **Max Dilendorf**

Partner

 [md@dilendorf.com](mailto:md@dilendorf.com)

 [@dilendorf\\_law](#)