

**DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N. Y. 10013
(212) 335-9000**



ALVIN L. BRAGG, JR.
DISTRICT ATTORNEY

January 26, 2026

Senator Chuck Schumer
322 Hart Senate Office Building
Washington, D.C.
20510

Senator Kirsten Gillibrand
478 Russell Senate Office Building
Washington, D.C.
20510

Senator Mark Warner
703 Hart Senate Office Building
Washington, D.C.
20510

Re: Stablecoin Legislation

Dear Senators Schumer, Gillibrand, and Warner,

I am writing to you regarding certain significant concerns we have identified with the current statutory regime governing “stablecoins.” *See* GENIUS Act of 2025, Pub. L. No. 119-27, 139 Stat. 419 (the “Genius Act”). Since being signed into law, the Genius Act has provided stablecoins and stablecoin issuers the imprimatur of legitimacy, while still allowing issuers to avoid significant regulatory requirements that are needed to combat financing terrorism, drug trafficking, money laundering, and especially cryptocurrency fraud. Notably, the Genius Act does not contain any provisions requiring stablecoin issuers to return stolen funds, or the proceeds of such funds, to victims. The failure of the Act to address this issue will result in victims with no recourse for recovering their losses. Issuers, on the other hand, are permitted to keep and generate interest from the stolen funds and criminal proceeds they control, and some issuers are currently using that loophole to literally profit from the criminal activity their cryptocurrencies facilitate.

Background

As you are well aware, there is currently a multi-billion cryptocurrency fraud industry targeting United States citizens which has increased exponentially over the last few years. *From Wall Street to Web3: Building Tomorrow’s Digital Asset Markets Before the US Comm. on Banking,*

Housing, and Urban Affairs, 119th Cong (July 9, 2025) (statement of Jonathan Levin, CEO Chainalysis Inc.) (estimating that digital assets received by illicit actors exceeded \$51 billion in the last year); (statement of Elizabeth Warren) (noting that the FBI estimated \$9 billion in cryptocurrency fraud in 2024); David Yaffe-Bellany, Spencer Woodman & Sam Ellefson, *The Crypto Industry's \$28 Billion in 'Dirty Money,'* N.Y. Times, November 17, 2025, <https://www.nytimes.com/2025/11/17/technology/crypto-exchanges-dirty-money.html>. Stablecoins have quickly become the cryptocurrency of choice for these criminal actors, as well as other transnational criminal organizations, including those engaged in financing terrorism, drug trafficking, and money laundering. In fact, stablecoins are estimated to now account for 63% of all on-chain criminal activity: literally billions of dollars in criminal transactions. Chainalysis 2025 Crypto Crime Report.¹ The trend line for the use of stablecoins in criminal transactions suggests that this percentage – and the amount of fraud – will continue to rise dramatically over the next few years. The overwhelming majority of these transactions are conducted in just two stablecoins: USDT and USDC, both of which are pegged to the United States dollar (“USD”).

USDT, managed by Tether Limited (“Tether”), and USDC, managed by Circle Internet Financial LLC (“Circle”), are the two largest stablecoins. USDT is the largest stablecoin and fourth largest cryptocurrency by market capitalization, with a total value of approximately \$186 billion in circulation. USDC is the second largest stablecoin and seventh largest cryptocurrency by market capitalization, with a total value of approximately \$74 billion in circulation. Circle and Tether are themselves each larger than the next-largest 100 stablecoin issuers combined.

Law enforcement, including the undersigned, regularly investigate criminal enterprises which use stablecoins to commit cryptocurrency fraud and launder stolen proceeds, among other crimes. Whenever possible, we attempt to freeze and seize stolen funds and proceeds and return such funds to victims through appropriate legal process. In the vast majority of cryptocurrency fraud investigations conducted by my office last year, stolen funds were converted, at some point, into USDT or USDC.

Circle claims to be an ally in this fight – but its practices tell a different story. In a hearing before the House Committee on Financial Services, Circle Director Caroline Hill stated that “[s]ince its founding, Circle has made combating illicit finance activities a foundational principle.” *Crypto Crime in Context Part II: Examining Approaches to Combat Illicit Activity Before the United States House Financial Services Committee, Subcommittee on Digital Assets, Financial Technology, and Inclusion*, 118th Cong. (Feb. 15, 2024) (statement of Caroline Hill, Senior Director of Global Policy and Regulatory Strategy). In reality, however, Circle seems more of an adversary in law enforcement’s fight against cryptocurrency fraud and to make victims of fraud whole, more aligned with the criminals conducting the fraud than law enforcement trying to prevent it.

In particular, Circle has refused to cooperate with law enforcement or freeze assets unless compelled to do so by legal process, refused to comply with validly issued state search warrants, and refused to return stolen funds to victims, even when compelled by court order.

¹ Available at <https://go.chainalysis.com/2025-Crypto-Crime-Report.html>, last accessed August, 7, 2025.

This is in stark contrast to any other regulated financial institutions, which respect formal requests from a law enforcement agency to temporarily freeze funds which are suspected of being stolen or proceeds of a crime while legal process is sought. Circle's refusal to respond to law enforcement requests to freeze assets, results in virtual assets to be moved, converted, and hidden, making recovery on behalf of a victim impossible. Circle's motive for not proactively assisting law enforcement and enabling cryptocurrency fraud appears simple: it has made millions, if not billions, by prioritizing profit over victims.

Tether, unlike Circle, has frozen stolen funds at the request of law enforcement and facilitated the return of such stolen funds to victims - *in some cases*. They only have done so, however, voluntarily, on an ad-hoc basis, and under the aegis of federal law enforcement. Tether disclaims any formal legal obligation to respond to state legal process, and has reserved the right to stop replying to law enforcement requests and warrants, or refusing to comply on a particular case, at their complete discretion. In freezing and returning stolen USDT, law enforcement has been left to Tether's mercy.

Tether

Based upon its protocol, and unlike other cryptocurrency issuers, Tether has the ability to both freeze and burn USDT. Specifically, Tether can freeze, or blocklist, any address containing USDT by preventing it from conducting any other future transaction on the blockchain. This literally holds the USDT in its current address and renders the USDT in that address valueless since it cannot be transferred to another other party. Tether can do this despite not having the private keys for a given address. This is significant because, as a result, Tether can freeze USDT held in any unhosted wallets. Additionally, Tether can also "burn" frozen USDT, removing the coin from circulation entirely, and then reissue a new coin in the same amount of USDT into an address that it, Tether, controls. This process is called a "burn and reissue." Because of their unique protocol, Tether has the ability to fully respond to search warrants and provide an identical value of substituted USDT to law enforcement.

At present, however, there is no statutory requirement for Tether to do so, nor any guarantee that Tether will continue to do so in the future. Rather, Tether, represents that they will "voluntarily" freeze USDT addresses at the request of law enforcement only when it makes a calculation that the "risk of freezing is within our risk tolerance" and only on the provision of detailed information concerning the underlying investigation, including:

- A narrative of the theft;
- The transaction hashes associated with the theft;
- The specific deposit addresses associated with the theft, including the victim addresses;
- Time and dates the theft occurred;
- The jurisdiction the victim(s) resides in;
- Measures used to verify the victims claim;

- Off-chain intelligence supporting your suspicions (redact details if needed);
- A visual representation of the flow of funds, including comments that explain tracing through service addresses, bridges, and mixers;

This information Tether requires includes highly personal information about the victim, the methods of law enforcement, the substance of grand jury investigations, and the identity of suspects. In many cases, some or all of this information cannot legally be disclosed under New York’s Grand Jury secrecy laws. See N.Y. Crim. Proc. Law § 190.20(4)(a). Even if this information can be provided by law enforcement, however, Tether makes clear that they reserve the right to deny a freeze request, reserving complete unilateral discretion in deciding whether to comply with the request – or not. Indeed, Tether also rejects the notion that they can be compelled to answer any U.S. based legal process given that they “do[] not operate in the U.S. and ha[ve] no offices in the U.S.”

Law enforcement has been able to convince Tether to freeze and reissue stolen funds in some cases, but only when operating in tandem with the federal government. Tether frequently trumpets these instances as examples of their cooperation with law enforcement. As a matter of policy, however, Tether denies any obligation to do so, claiming that, absent their voluntary cooperation, the only way stolen USDT in unhosted wallets can be returned to victims is to “apprehend a suspect, and obtain the private keys.” In many instances, apprehending a suspect and obtaining the private keys is simply not feasible. For example, this would require law enforcement to: (1) identify the suspect, (2) locate the suspect, (3) determine that the suspect’s location is in a jurisdiction that will cooperate with U.S. law enforcement, (4) identify the location the suspect used to commit the crime and/or currently possesses computer equipment, (5) obtain an MLAT to search that location and seize certain evidence, (6) hope that the suspect does not move or change locations in the many months it takes to obtain the MLAT, (7) hope that the private keys located in the target location are in an unencrypted device or in hard copy, (8) hope that investigators are able to locate and obtain those private keys during the execution of the warrant. Given the prevalence of cryptocurrency fraud originating in jurisdictions that will not cooperate with U.S. law enforcement (i.e. China, North Korea, Russia), the likelihood of obtaining the private keys to given USDT addresses in most cryptocurrency fraud investigations is close to zero.

The reality for many victims, therefore, is that funds stolen in or converted to USDT will never be frozen, seized, or returned. Moreover, although Tether may freeze, burn, and reissue USDT at the request of law enforcement in some limited circumstances, they acknowledge no legal obligation to do so. They currently decide on a case-by-case basis when they will assist law enforcement in recovering funds for victims, and nothing prevents them from stopping all reissuance entirely.

Circle

Circle is a publicly traded company domiciled in Delaware, headquartered in New York City, and registered with FinCEN and the New York State Department of Financial Services.

Circle repeatedly claims to be an ally in the fight against financial fraud. Their policies, however, are significantly worse than those of Tether for victims of fraud.

Circle, like Tether, has the ability to freeze USDC, but they disclaim any ability to burn and reissue frozen funds and claim that they cannot do so under their protocol.² Unlike Tether, however, Circle refuses to temporarily freeze funds at the request of law enforcement, and will only do so after they have received a signed judicial order or warrant. Given the speed at which criminals and criminal networks operate, by the time it takes to obtain an order or warrant to freeze a given USDC address, the funds at issue have often already been moved to a different address, or been converted to a different virtual currency. As a result, Circle's refusal to accept a formal letter from law enforcement to temporarily freeze USDC while a warrant is obtained greatly hinders law enforcement's ability to recover stolen funds, prevents stolen funds from being laundered, and increases the loss to victims as the stolen funds are successfully moved overseas, converted to a different cryptocurrency, or otherwise hidden outside the reach of law enforcement.

Even when funds are successfully frozen, Circle will not voluntarily return the funds, or a USD equivalent of said funds, to victims, and have refused to honor New York State court orders commanding the same. In almost every state case, therefore, stolen USDC will simply remain frozen and under the complete control of Circle but not be returned to any victims.

In a recent matter being handled by the New York County District Attorney's Office ("DANY"), Circle indicated it would agree to return the USD equivalent to victims only if the underlying frozen USDC were forfeited pursuant to a federal or state forfeiture action.³ Rather than pursue enforcement of our warrant or a contempt proceeding, DANY collaborated with federal authorities in the Southern District of New York and obtained federal forfeiture of the USDC at issue. However, once that process was completed, Circle reneged on their agreement, and failed to return the stolen funds to victims despite a judgment of forfeiture signed by a federal judge.

Even were Circle to have complied with its own suggested course of action – and they have not – it is not feasible for state and local law enforcement agencies to obtain the assistance of the Department of Justice on each and every case. The federal government cannot act as a proxy or clearinghouse for all forfeiture actions sought by State or local law. The reality, therefore, is that USDC may be able to be frozen on the blockchain, but Circle will not help victims of fraud receive a single cent in restitution.

Financial Incentives for Frozen Stablecoins

Circle's "freeze but don't reissue" policy has resulted in a relatively high amount of "frozen" stablecoins, but only a negligible amount of funds have actually been returned to

² The protocol that Circle uses is one of its own design and in making it, intentionally decided to not include this functionality, unlike that of Tether. It is unclear if Circle has the ability to update and change their protocol for USDC to also permit burning addresses.

³ Significant limitations in New York State's own forfeiture law will preclude forfeiture actions virtually every cryptocurrency fraud case.

victims. While devastating to victims, their internal practices have resulted in a financial windfall for Circle.

Both Tether and Circle claim to hold USD reserves equivalent to the USDT and USDC in circulation. Contractually, they are required to allow customers to redeem that USDT and USDC on demand, requiring them to maintain sufficient liquidity to pay out on future claims. Nonetheless, despite these commitments, public records and reporting reveal that in 2024, Circle and Tether each made in excess of one billion dollars of profits which was derived solely from investing their reserve funds: including reserve funds backing stolen and frozen USDC.

As explained above, Circle will freeze USDC in response to a warrant. Since the frozen funds are not able to be redeemed by any party, Circle collects interest on the underlying reserve funds during the entire time they are frozen without any risk of redemption. Given this fact, Circle's motive for not assisting law enforcement becomes crystal clear: it is financially preferable to only freeze cryptocurrency deemed to have been stolen, but not return the underlying asset to law enforcement or any fraud victim, because Circle can continue to collect the interest through investment of the underlying funds.

The amount of frozen funds is massive and has grown quickly. For example, while Circle publicly reported just \$100,000 in frozen USDC in January 2021, this amount ballooned to \$2.6 million January 2022, then almost tripled to \$6.4 million by January 2023. By January 2024, it was more than 10-times that amount, at \$78 million. As of November 2025, the amount of frozen funds which Circle is profiting from is more than \$114 million. See <https://www.circle.com/transparency#stability> (last accessed November 12, 2025).

Despite the significant profits Circle has been making by holding these stolen funds, Circle refuses to assist law enforcement in returning stolen funds to victims. Earlier this year, Circle formally refused to honor New York State warrants and court orders compelling them to return the stolen funds or proceeds to victims – and hired outside legal counsel to challenge the search warrants seeking their return. Circle apparently prefers to have millions in their own pocket, earning interest, then return stolen funds and their proceeds to the victims of crime. Not only is Circle refusing to help fraud victims by returning stolen funds to them, but Circle is literally making money on their backs.

These numbers will only continue to increase exponentially as USDC becomes more mainstream and, as a result, more and more stolen funds and proceeds are frozen – allowing Circle to continue to earn interest on increasingly larger amounts of stolen funds. In the near future, we believe that Circle will make hundreds of millions in profit solely by retaining possession of the reserve assets backing stolen funds, all while victims receive no restitution whatsoever – and in contravention of court orders to return such funds.

The Genius Act

Unfortunately, the current text of The Genius Act enshrines these practices into law. While the Act has some limited provisions that may assist federal law enforcement in freezing stablecoins, it actually makes freezing stablecoins harder for *state and local* law enforcement. Even more troubling, the Act has no provisions whatsoever which compel, let alone mention, the return of stolen funds or proceeds to fraud victims. The Act is therefore a net negative for

cryptocurrency fraud victims and a significant missed opportunity to redress the wrongful practices of the stablecoin industry, which will only worsen as time goes on.

With respect to freezing, the Genius Act provides that stablecoin issuers must comply with “any lawful order,” defined, in part, as an order issued “under Federal law” to “seize, freeze, burn, or prevent the transfer of payment stablecoins issued by the person.” Genius Act. Sec. 2(16), 4(6). This provision is deficient in two primary ways:

- (1) Under the Genius Act, stablecoin issuers are only required to comply with orders “under Federal law;” it says nothing about complying with lawful state court orders. Given that the Genius Act only requires compliance with federal orders, it suggests that stablecoin issuers do not need to comply with any lawful state-issued court freeze orders. As such, state law enforcement may now be in an even worse position when seeking to freeze stablecoins than before passage of the Genius Act. Given their current response to state law enforcement requests, we believe it likely that Tether and Circle will look to this provision in the future to further limit their support of state and local law enforcement and citing to this omission in the statute.
- (2) Given the speed of cryptocurrency transactions, many cryptocurrency exchanges voluntarily freeze suspected stolen proceeds upon the request of law enforcement for a limited period of time until a warrant can be secured. This is because all of the stakeholders recognize how quickly stolen funds and proceeds can be moved and laundered, making them unavailable for possible seizure. The Genius Act contains no provision for emergency or non-judicial freezing of stablecoins; it only obligates stablecoin issuers to freeze assets when they are obligated to do so by a formal Federal court order. Many statutes contain exceptions for emergency or expedited action under certain circumstances, and the Genius Act should have as well.

As limited as the Genius Act is with respect to freezing stolen stablecoins, it is immeasurably worse with respect to returning such stolen funds or proceeds to victims of fraud. The statute is devoid of any language regarding returning stolen funds to victims pursuant to judicial order or otherwise. The absence of any language in the statute will embolden stablecoin issuers, and even provide legal cover, when they affirmatively decide to keep stolen funds and proceeds under their control rather than returning them to victims. Although the rights of victims were discussed during debate on the Genius Act, for reasons that are unclear, language addressing the return of stolen funds never made it into the bill. See 171 Cong. Rec. H3257 (July 15, 2025) (statement of Rep. Scanlon) (noting that the Genius Act “will leave regular investors on the hook if they are victims of fraud”); 171 Cong. Rec. S3329 (June 11, 2025) (statement of Sen. Warren). This omission is particularly unusual given the explicit requirement in the Act that a stablecoin issuer be able to *freeze* stablecoins upon court order. If there is no coordinate requirement for the funds underlying the frozen or burned stablecoins to be returned to a victim, this will simply allow stablecoin issuers to indefinitely hold the reserve funds for themselves and profit on the backs of individual victims. Indeed, this is exactly what Circle is already doing today.

Conclusion

The United States is in a uniquely advantageous position in combatting terror financing, money laundering, cryptocurrency fraud, and illicit finance flows. Stablecoins have quickly become the most important cryptocurrency for criminal actors and the two largest issuers (Circle and Tether) are either based in the United States or have otherwise made themselves subject to our laws. Unlike any other type of cryptocurrency, Circle and Tether have the ability to freeze stablecoins in unhosted wallets and therefore a unique ability to immediately halt the flow of stolen funds and criminal proceeds. Rather than act on that ability to help victims of fraud, Tether has provided assistance only in limited circumstances, and Circle has chosen to actively thwart law enforcement and to profit from victims' losses.

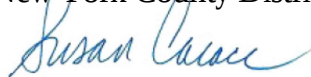
Unfortunately, the Genius Act only exacerbates this problem. It does not obligate any stablecoin issuers to comply with federal, state or local law enforcement requests to freeze, seize, and return stolen funds. As a result, victims across the United States lose everything, while Circle and Tether generate hundreds of millions in profits. Law enforcement's limitations has not gone unnoticed and the use of USDT and USDC stablecoins by transnational criminal enterprises, has grown dramatically over just the last few years.

Tether, and especially Circle, are profiting from fraud. Unfortunately, the Genius Act, in its current form, enshrines some of their current practices in law. As such, I welcome any opportunity to help modify this statute or enact additional laws to more robustly support criminal investigations and to aid victims of crime which involve stablecoins.

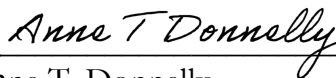
Sincerely,



Alvin Bragg
New York County District Attorney



Susan Cacace
Westchester County District Attorney



Anne T. Donnelly
Nassau County District Attorney



Letitia James
Attorney General of New York



Melinda Katz
Queens County District Attorney