Wave
Digital Assets

Nicole Trudeau, Esq.
General Counsel
Wave Digital Assets LLC
11740 San Vicente Blvd.
Suite 109-632
Los Angeles, CA 90049

January 27, 2026

Mr. William M. Blier
Deputy Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

URGENT FORMAL COMPLAINT AND REQUEST FOR INVESTIGATION: Ongoing Risk to Seized Cryptocurrency Arising from Documented USMS Procurement Failures

Dear Deputy Inspector General Blier,

I write on behalf of Wave Digital Assets LLC ("Wave"), in my capacity as General Counsel, to submit this formal and urgent complaint regarding credible public allegations that more than $40 million in seized United States government cryptocurrency has been unlawfully transferred from government-controlled wallets. These allegations reveal serious and unremedied failures in the United States Marshals Service's ("USMS") procurement, contractor-selection, and oversight processes for cryptocurrency custody. These failures not only permitted the alleged loss to occur, but continue to expose government-held digital assets to immediate, foreseeable, and preventable compromise.

This complaint is submitted as a continuation and escalation of concerns previously raised with your Office. In December 2024, Wave's Co-founder, Les Borsai, formally contacted the Office of the Inspector General to warn that the USMS cryptocurrency procurement, particularly with respect to higher-risk "Class 2–4" assets, suffered from fundamental control deficiencies, misaligned procurement criteria, and the selection of unlicensed vendors for highly regulated activities. That correspondence is attached as Appendix A.

Recent investigative reporting and independent blockchain-forensic analysis, detailed in numerous articles attached as Exhibit A, describe a scheme in which an individual allegedly boasted on Telegram about accessing and draining wallets associated with U.S. government seizures, activity that ultimately enabled investigators to trace on-chain transactions back to USMS seized assets. The claimed losses from this alleged theft are immense, estimated to be tens of millions of U.S. dollars, although the exact full scope of loss is not yet known. Such a loss under the management of a government contractor would be troubling on its own, but the

alleged identity of the apparent perpetrator makes this matter of the utmost alarm. Public reporting further indicates that the individual allegedly responsible is closely related via familial connection to a principal associated with Command Services & Support ("CMDSS"), the very contractor selected by USMS to manage higher-risk Class 2–4 seized digital assets. These allegations are not mere Internet rumormongering. Law-enforcement investigations are reportedly ongoing at this very moment due to the seriousness and credibility of the claims in question.

If substantiated, these allegations would constitute one of the most significant failures of seized-asset custody in United States history. Critically, however, this outcome was expressly foreseeable and repeatedly identified in advance by Wave during the USMS procurement process, by Wave's Co-founder in direct correspondence to this Office in December 2024, and by the OIG itself in prior findings concerning internal controls and contractor oversight. These risks were not theoretical or novel. Rather, they reflected known control deficiencies and procurement weaknesses that went unremedied, despite clear notice.

What has now occurred appears to be the direct and preventable consequence of the failure to implement corrective measures previously identified by this Office and reinforced by regulated market participants, resulting in a breakdown of safeguards over digital assets purportedly "safeguarded" by USMS.

I. Wave Digital Assets and Relevant Expertise

Wave is a registered investment adviser, regulated by the Securities and Exchange Commission ("SEC") under the Investment Advisers Act of 1940, a statute enacted specifically to prevent fraud, insider abuse, and the misappropriation of entrusted assets. Since 2018, Wave has specialized in fiduciary management, valuation, governance, and lawful liquidation of digital assets under relevant compliance regimes designed to mitigate precisely the risks now alleged.

Wave has provided education, forensic support, and seized-asset advisory services to federal and state agencies. We participated fully in the USMS procurement process for Class 2-4 seized cryptocurrency management under solicitations 15M50023QA4400002 and 15M50023QA4400003. As detailed both in our formal bid protests and in our December 2024 letter to the OIG, we concluded that the procurement framework was fundamentally flawed and expressly warned that USMS's chosen approach created material and foreseeable risk to government-held digital assets.

II. A Prolonged Pattern of Procurement Mismanagement

Public records and reporting reflect that the USMS has struggled for nearly seven years to establish a stable, competent framework for managing seized cryptocurrency:

- **2018:** USMS sought external assistance following internal control deficiencies identified by the OIG.
- **April 2021:** Contract awarded to BitGo, later rescinded after USMS determined the firm did not qualify as a required "small business."
- **July 2021:** Award shifted to Anchorage Digital, which was subsequently deemed ineligible under the same small business criteria.
- **2024:** USMS abandoned its unified custody model and split responsibility into multiple classes:
    - **Class 1 assets** (exchange-supported, cold-storage assets such as Bitcoin and Ether) awarded to Coinbase; and
    - **Class 2–4 assets** (complex, illiquid, or protocol-specific tokens) awarded to CMDSS, a general technology services vendor.

As emphasized in Wave's December 2024 correspondence to this Office, these repeated reversals and restructurings reflect persistent institutional uncertainty regarding the nature of digital assets, the regulatory regimes governing them, and the expertise required to safeguard them.

Indeed, going all the way back to 2022, your very Office conducted an audit of the USMS' management of seized cryptocurrency. This audit observed that "the USMS faces challenges in managing and tracking cryptocurrency in the U.S. Department of Justice's (DOJ) official seized asset tracking system." It further noted that "These deficiencies risk an inaccurate accounting of cryptocurrency in USMS custody and the potential for a loss of assets." The audit further stated that "the USMS should establish seized cryptocurrency policies and procedures related to inventory management, asset storage, quantification, valuation, and disposal prior to handing over its seized cryptocurrency responsibilities to a contractor." It appears, unfortunately, that the USMS failed to achieve this goal.

III. Wave's Protest and Ignored Warning Signs

Wave competed directly against CMDSS for management of the Class 2–4 assets and ultimately lost the award. Wave's protest, consistent with concerns previously raised to the OIG, identified concerns that recent events now render acute, including that:

- CMDSS is not licensed with the SEC or the Financial Industry Regulatory Authority, notwithstanding that many Class 2–4 assets implicate securities-law obligations and require regulated fiduciary handling;
- USMS failed to meaningfully investigate or resolve an apparent conflict of interest arising from CMDSS's employment of a former USMS official with access to non-public procurement and asset-management information;
- The procurement reflected a fundamental mischaracterization of digital assets, treating them as static physical property rather than as bearer instruments requiring continuous technical controls, segregation of duties, and insider-risk mitigation.

Multiple bidders raised these deficiencies during the procurement process. Wave, in particular, presented demonstrably superior technical capabilities, proposed to perform the work at a lower cost, and structured its bid around licensed, regulated fiduciaries and auditable internal controls consistent with federal expectations for safeguarding high-risk government assets.

Wave, as mentioned above, is an SEC-registered investment adviser and proposed custody through BitGo Bank & Trust, National Association, which is now a federally chartered trust bank regulated by the Office of the Comptroller of the Currency and subject to SEC oversight as a publicly-traded company. This structure provided clear accountability, segregation of duties, personnel vetting, and enforceable compliance obligations.

By contrast, CMDSS and its proposed subcontractors lacked comparable regulatory licenses, fiduciary duties, and supervisory regimes. CMDSS was nevertheless still entrusted with attempting to safeguard bearer digital assets uniquely susceptible to insider abuse despite this precise combination of conditions. This is the precise combination of conditions that OIG guidance has repeatedly identified as indicators of both elevated fraud and misappropriation risk.

IV. Ongoing Risk and Continuing Exposure

If the reported facts are accurate, CMDSS may continue to exercise custody or access over forfeited United States government digital assets notwithstanding the alleged breach (and, potentially, multiple breaches, based on the reporting that has been done). So long as CMDSS remains a USMS contractor and these assets are not affirmatively transferred to a secured, independently supervised custodial environment, the risk of additional loss remains active and unmitigated.

Under established OIG oversight principles, the continuation of contractor access following a credible compromise constitutes a high-risk condition of foreseeable and preventable harm, warranting immediate remedial intervention.

V. Personnel Vetting and Access-Control Failures

Publicly available arrest records further indicate that the individual alleged to have accessed and misappropriated seized assets has been arrested multiple times, raising grave concerns regarding contractor personnel vetting, access authorization, and USMS supervisory controls. Relevant records are included as Exhibit B.

VI. Relevant Contract Language

It is worth observing that, if the allegations are substantiated, CMDSS has, at best, completely failed in its obligations under the contract. It hardly needs to be stated that, if CMDSS were

directly involved in the alleged misappropriation, such would be a serious crime. But, even were it not, it has completely neglected its duties to the substantial loss of the U.S. government.

The solicitation for this contract stated that the "USMS expects the Contractor, as its agent, to take prudent action and good faith on the USMS's behalf with the same duty of care while augmenting our capacity and efficiency regarding the custody, management, and disposal of cryptocurrency." Solicitation PWS at 4. It required the contractor to, among other things, "provide all aspects of secure storage and management of cryptocurrency in its custody from the time of receipt until disposal." Id. at 6. "All cryptocurrency assets shall be backed up in redundant geographically separate logical locations, minimum 100 miles, and in a manner that prevents compromise by internal collusion, third party collusion, remote or local cyber-attacks, physical loss, fire or acts of nature." Id. at 7. Plus, the contractor "shall take prudent steps to prevent the loss of Government cryptocurrency assets including but not limited to theft, human error, system failures, bankruptcy, and acts of nature." Id. at 9. Clearly, security of cryptocurrency was an essential element of the contract.

The solicitation for the contract also contained DJAR-PGD-08-04, "Security of Systems and Data, Including Personally Identifiable Information Security of Systems and Data, Including Personally Identifiable Data." This clause states, in relevant part,

> By acceptance of, or performance on, this contract, the contractor agrees that with respect to the data identified in paragraph a, in the event of any actual or suspected breach of such data (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), the contractor will immediately (and in no event later than within one hour of discovery) report the breach to the DOJ CO and the contracting officer's technical representative (COTR).

Solicitation at 7.

The solicitation also contained DOJ-05, "Security of Department Information and Systems." This clause observes that "Section 2839.102 of the Justice Acquisition Regulation (JAR), (48 C.F.R. § 2839.102), applies to this contract. Accordingly, all contractors are obligated to comply with all applicable DOJ security policies, directives, or guidance documents, including the security requirements in the provisions in this contract clause." That an individual was apparently able to abscond with tens of millions of dollars in cryptocurrency on apparently multiple occasions is a tremendous failure to abide by these policies, to say the very least. Certainly, such incidents should at least have been observed and reported to the government soon after their occurrence. Indeed, the clause notes that "The Contractor shall immediately (and in no event later than 1 hour of discovery) report any Confirmed Security Incident to the DOJ CO and COR." This apparently was never done. In such extreme circumstances, while it again hardly needs repeating to the government, FAR 9.406-2(c) observes that "The suspending and debarring

official may debar— A contractor or subcontractor based on any other cause of so serious or compelling a nature that it affects the present responsibility of the contractor or subcontractor." Considering the enormity of the loss and the circumstances surrounding the same, even if CMDSS was not directly involved in this incident, such extreme and gross negligence should at the very least warrant consideration of debarment or suspension.

VII. Urgent Need for OIG Action

This matter presents an immediate and continuing threat to public assets. The same structural deficiencies that permitted this alleged loss may still exist today.

Wave therefore respectfully and urgently requests that the Office of the Inspector General:

1. Initiate a formal investigation into the alleged misappropriation and any continuing exposure of seized digital assets;
2. Determine whether additional government-held cryptocurrency remains at risk under current custody arrangements;
3. Examine USMS procurement, conflict-of-interest review, licensing determinations, and contractor oversight practices;
4. Assess whether the current contract should be terminated for default and CPARS ratings should be determined to be Unsatisfactory;
5. Assess whether the current contractor should be investigated for debarment and for being nonresponsible; and
6. Consider immediate interim measures to secure seized digital assets pending the outcome of the investigation.

Wave submits this complaint in good faith and in the interest of preventing further harm to the United States. We stand ready to provide briefings, documentation, or technical assistance at your request.

Respectfully submitted,

Nicole Trudeau, Esq.
General Counsel
Wave Digital Assets LLC

Appendix A

Letter from Wave Co-Founder Les Borsai to the Office of the Inspector General in December 2024 (begins on next page):

Wave
Digital Assets

I am the co-founder of Wave Digital Assets (Wave), a registered investment advisor specializing in cryptocurrency. Wave is a SEC-registered investment advisory firm that provides a unique combination of venture capital, fund, and private wealth management to the digital asset ecosystem. Founded in Los Angeles in 2018 by a team of highly experienced crypto natives and financial services professionals, Wave brings together smart capital strategies, deep institutional expertise, and cutting-edge ideas to help investors unlock the potential of digital assets. Wave has deployed over $2B in AUM and is registered with the US Securities & Exchange Commission as an investment adviser. Over two years ago, we shifted our focus to government practice, establishing contracts with multiple state and federal agencies.I am writing because I am deeply concerned about the USMS procurement processes related to the management of cryptocurrencies (solicitations 15M50023QA4400002 and 15M50024QA4400003). Based on our recent experiences, I believe these processes were fundamentally flawed, potentially causing significant harm to the U.S. government and, by extension, the public interest.

We recently expressed our concerns via an agency-level post-award protest, during which we hoped to achieve a constructive dialogue with USMS by engaging with them. However, the Contracting Officer's response did not address any of our questions and further amplified our concerns.

In light of the gravity of these issues and your Office's prior report on the USMS' handling of cryptocurrency from 2023, I felt compelled to reach out to you directly as we consider our legal options, including proceeding to a GAO protest or pursuing litigation in the Court of Federal Claims.

Wave Digital Assets has been deeply involved in USMS cryptocurrency-related activities, participating in the RFI and RFP processes for "Class 1" (awarded to Coinbase) and as a finalist for "Classes 2-4." Despite our qualifications—including successfully liquidating over $2 billion in "Class 2-4" assets under SEC fiduciary standards—the recent contracting decisions raise critical questions about the process, the expertise of key personnel, and the adherence to legal and industry standards.

On June 14, 2022, your office issued a report examining the USMS management of seized cryptocurrency and found numerous issues, including:

- **Lack of Comprehensive Inventory Management**. DOJ's official seized asset tracking system does not have the necessary functionality to enable daily management of cryptocurrency assets. As a result, the USMS was using supplemental spreadsheets to track cryptocurrency assets, which lacked documented operating procedures and other inventory management controls risking an inaccurate accounting of cryptocurrency. In fact, we found that the inventory spreadsheets contained inaccuracies.
- **Inadequate, Incomplete, and Conflicting Policies and Procedures**. The USMS did not have adequate policies related to seized cryptocurrency storage, quantification,

valuation, and disposal, and in some instances, guidance was conflicting. For example, we found that the USMS policy did not have an established process for recording new cryptocurrency assets created after a "fork" (whereby a single cryptocurrency splits into two separate cryptocurrencies). As a result, the USMS may fail to identify and track forked assets, and thereby lose the opportunity to sell those assets when they are forfeited.

- **Outsourcing Management of Seized Cryptocurrency**. The USMS is in the process of awarding a contract to outsource the management of its seized cryptocurrency, which we believe will assist the USMS in addressing some of the issues we identified. However, we believe it is imperative that the USMS establish properly documented policies and procedures prior to handing over cryptocurrency responsibilities to a contractor, as doing so will best prepare the USMS to ensure that the future contractor's services meet the USMS's needs and expectations.

As you know, and as your office previously pointed out, cryptocurrencies (digital assets) are a relatively new, complicated, and evolving asset class that require specialized care and knowledge to properly manage. In particular, the "Classes 2-4" procurement involves the management and liquidation of very specialized assets that the SEC would consider "securities" (which is not likely to change even with the new administration).

While we understand the USMS were incentivized to act quickly in light of your Office's report regarding their handling of cryptocurrencies, we believe this may have led to a short-sighted and myopic process that entirely overlooked the highly-regulated nature of the Class 2-4 asset classes, and reflects a wholesale misunderstanding of what industry standard practices look like for assets of this nature. This is problematic in terms of its potential mishandling of these critical assets and the federal government having potentially engaged vendors that are acting illegally – a concern that your office would view as significant.

For example, a critical portion of the Class 2-4 services involves the liquidation of the assets. The SEC views this as asset management activity, yet the USMS has selected unlicensed and inexperienced vendors to engage in this highly-regulated activity (in contravention of US securities laws).

As another example, Classes 2-4 assets often have very unique attributes that can easily lead to major losses if handled improperly, and limited options for liquidity when the USMS are seeking to dispose of the assets. Having liquidated over $2 billion in Class 2-4 assets in line with fiduciary standards under SEC rules, we are authorities on how complicated it is to manage and how difficult it can be to liquidate these assets. It has taken us many years with highly-specialized and trained teams to acquire the knowledge and experience required to manage these assets properly. The awardee and its subcontractors simply do not have this experience.

It should be noted that the RFP did not speak whatsoever to any securities-law requirements or considerations, and our inquiry with the Contracting Officer regarding the proper licensing of the selected vendors was summarily dismissed as irrelevant simply because the original (flawed)

RFP did not include a requirement that vendors be licensed to engage in the work required under the RFP's statement of work. This is very concerning to us and should be an area of inquiry for your office.

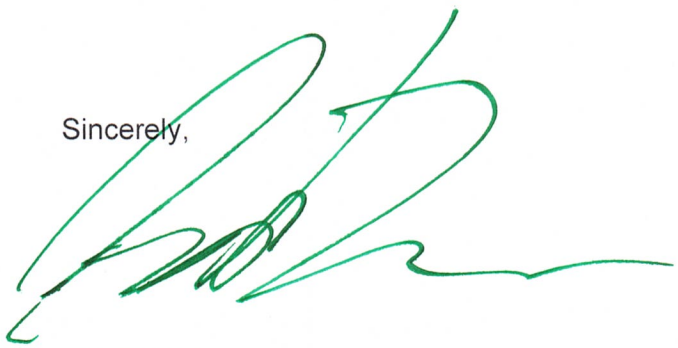
We have offered our services to the awardee in an effort to help mitigate these concerns, but they declined our invitation to meet. The urgency created by your Office's 2022 report on USMS cryptocurrency handling may have caused a rushed procurement process and appears to have resulted in critical oversights by the USMS. By failing to account for the highly regulated nature of these assets, the USMS risks both non-compliance with securities laws and substandard stewardship of public resources – in addition to not being in full compliance with your 2022 audit report.

In light of the above, and as we consider escalating our protest to the GAO or commencing litigation, I am urging your Office to review these procurement processes and their alignment with federal laws and standards. Our goal is straightforward: to ensure that the public interest is served by engaging qualified vendors operating legally and with the necessary expertise.

To assist your review, I am enclosing our submission, the award details, the debrief, and our agency protest. I welcome the opportunity to discuss this matter further and provide any additional context or assistance required to address these critical concerns.

Thank you for your attention to this urgent matter and we welcome the opportunity to meet and discuss our concerns with your office.

Sincerely,



Les Borsai

Co-Founder & Chief Strategy Officer
Wave Digital Assets

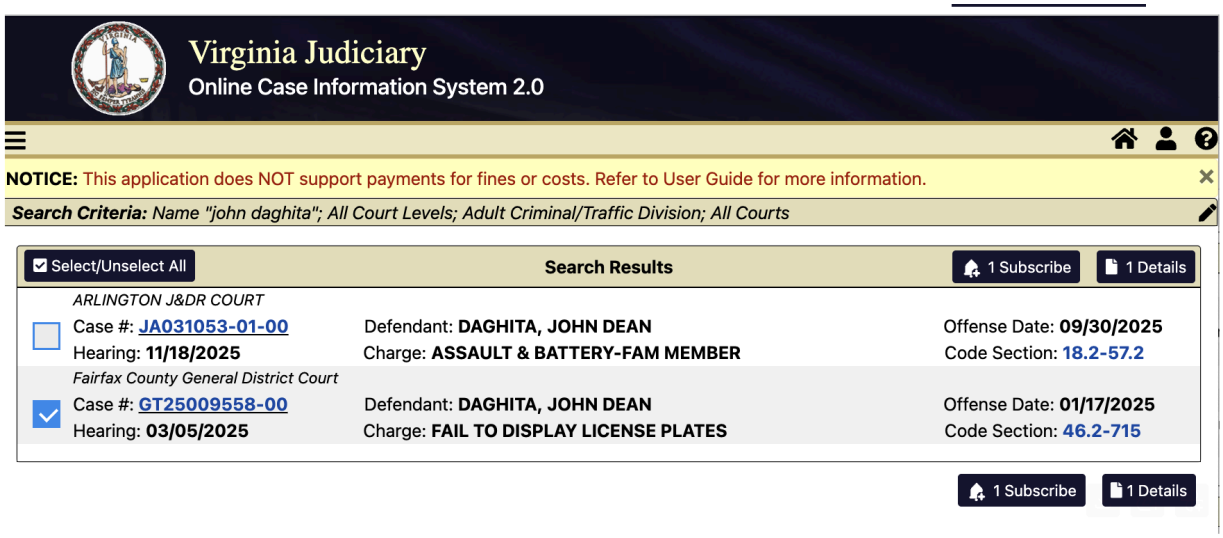
Exhibit A

Investigative news articles and blockchain-analysis reports describing the alleged misappropriation of seized government cryptocurrency.

1) Coindesk: U.S. Marshals investigate claims that son of government contractor stole $40 million of seized crypto
2) Bitcoin Magazine: US Government Investigating Alleged $40 Million Crypto Theft by Federal Contractor's Son
3) Yahoo Finance: Over 300K US Government Bitcoin at Risk After Alleged Insider Theft Exposes Custody Failures
4) The Block: Individual behind $40 million government wallet theft is son of seized-crypto contractor executive: ZachXBT
5) Yellow: ZachXBT: $40M Stolen From U.S. Marshals By Crypto Contractor's Son

Exhibit B

Publicly available arrest records relating to the individual alleged to have accessed and misappropriated the assets.



Virginia Judiciary
Online Case Information System 2.0

NOTICE: This application does NOT support payments for fines or costs. Refer to User Guide for more information.

Search Criteria: *Name "john daghita"; All Court Levels; Adult Criminal/Traffic Division; All Courts*

Select/Unselect All | **Search Results** | 1 Subscribe | 1 Details

ARLINGTON J&DR COURT

Case #: JA031053-01-00 | Defendant: **DAGHITA, JOHN DEAN** | Offense Date: **09/30/2025**
Hearing: **11/18/2025** | Charge: **ASSAULT & BATTERY-FAM MEMBER** | Code Section: **18.2-57.2**

Fairfax County General District Court

Case #: GT25009558-00 | Defendant: **DAGHITA, JOHN DEAN** | Offense Date: **01/17/2025**
Hearing: **03/05/2025** | Charge: **FAIL TO DISPLAY LICENSE PLATES** | Code Section: **46.2-715**

1 Subscribe | 1 Details