MALIA M. COHEN
CALIFORNIA STATE CONTROLLER

Request for Information

UPDRFI0125

for

Unclaimed Cryptocurrency Asset Management

October 29, 2025

Table of Contents

1.0 Purpose and Intent

The State Controller's Office (SCO) is seeking information regarding cryptocurrency custody platforms and related services for managing unclaimed crypto assets. This could be accomplished through a third-party custodian, implementing a direct custody model, or other proposed model.

These services will ultimately allow the State to achieve its goals of providing secure, compliant, and scalable custody solutions for unclaimed cryptocurrency assets, Non-Fungible Tokens (NFTs) and other emerging digital assets. This Request For Information (RFI) aims to explore custody, reporting, and asset transfer solutions to inform the State's management of digital wallets, adhering to all applicable legal and regulatory frameworks.

The response should provide clarity on options for both transferring control of entire wallets (private keys) and transferring assets from custodial wallets to claimants upon approved claim evaluation. The State of California also seeks insight into the future scalability and adaptability of the proposed solutions.

2.0 Objective

The objectives of this RFI are to:

1. Identify one (1) or more options that would support California's Unclaimed Property Program taking possession of unclaimed virtual assets and reuniting them with their owners.
2. Identify implementation options.
3. Identify different workflow options.
4. Broadly identify the range of costs and pricing models related to the above.

3.0 Background

3.1 Unclaimed Property Program

The California Unclaimed Property Program (Program) is part of a national effort that offers consumers a central location to search for financial assets left inactive by its owner for a period of time, typically three (3) years. The Program has been in existence since 1968 and is governed by California Code of Civil Procedures (CCP) 1500, Unclaimed Property Law (UPL). The UPL requires financial institutions, insurance companies, corporations, businesses, and certain other entities to report and submit their customers' property to SCO when there has been no activity for a period of time [generally three (3) years]. Common types of unclaimed property include but are not limited to bank accounts, stocks, uncashed checks, insurance benefits, wages, and safe deposit box contents. Property does not include real estate. It is the responsibility of the State Controller to safeguard lost or forgotten property for as long as it takes to reunite it with the rightful owners. There is no deadline for claiming property once it is transferred (escheated) to SCO, nor fees associated with

claiming this property. The UPL prescribes the circumstances under which intangible property escheats to the State, including how and when potential owners must be notified that their property is at risk of being escheated and the manner in which the escheated property must be delivered to SCO. Intangible property is only subject to the UPL if the apparent owner's last known address is within the state, if that address is unknown, or if there is another link to the state, as specified. Existing law provides how and when securities which are escheated to the State pursuant to the UPL may be sold and how the securities or funds from their sale may be returned to their owner.

3.2 Unclaimed Property Overview

Unclaimed Property is defined as, any intangible, and certain tangible, personal property that is statutorily deemed abandoned and cannot, for various reasons, be delivered to the rightful owner. Common examples include dormant bank accounts, safe deposit boxes with unpaid fees, utility deposits and refunds, uncashed checks, matured insurance policies, credit balances, etc. Businesses, non-profit organizations, and government entities (Holders) that possess or otherwise owe unclaimed property are required to report and remit the assets to the State every year. Until such property is claimed by the rightful owners or their heirs, it is safeguarded in the State's custody, Unclaimed Property Fund.

3.3 Holder Overview

California's UPLs require Holders to report and remit property to the state when they lose contact with the owner and/or the owner makes no indication of interest or knowledge of the asset; usually after a period of one (1) to three (3) years. Each year, the Unclaimed Property Division (UPD), Holder Operations Bureau (HOB), interacts with tens of thousands of businesses in California, the United States, and abroad. In general, the property owner's last known address determines the state to which the property is reported. In California, the Holder Notice reporting season occurs every November; the annual filing deadline is November 1 for each year ending as of the preceding June 30 or May 1 for life insurance. HOB provides tailored and expert advice on program requirements both during the reporting season and proactively throughout the year.

3.4 Claiming Property

As soon as UPD receives and verifies unclaimed property, the data becomes available on the SCO website for potential owners to identify and claim. The Consumer Services Bureau (CSB) is responsible for returning assets to their rightful owners or their heirs. The Support Services Bureau (SSB), Locator Unit, proactively looks for owners and assists them file a claim. The HOB, Outreach/Compliance Unit, actively participates in efforts to spread and promote greater awareness of the Program through multiple outreach and marketing efforts, and reunite owners with their property. When claims are received, UPD evaluates documentary evidence to ensure the rightful owners receive the correct amount of property from the state's custody.

3.5 Cryptocurrency

Although holders have not yet identified wallets containing NFTs as abandoned property, which may include various blockchains and standards, SCO anticipates this will occur in the near future. Given the potential for remittance of cryptocurrency, digital financial assets (DFA) from any blockchain or standard, the breadth of coverage required for the solution will be important for long-term planning.

This RFI seeks to identify solutions for securely storing and managing these DFAs, to include the process of reuniting them their rightful owners, in a manner that aligns and complies with the UPL and regulations of California.

At this time, the SCO current Assets Under Management (AUM) is $15.4 billion.

3.6 Legislation

The Program, administered by SCO under CCP 1500 et seq., is responsible for safeguarding lost or abandoned property until rightful owners can reclaim it. With the growing prevalence and adoption of virtual currencies such as Bitcoin and Ethereum, the State of California enacted Senate Bill (SB) 822 to provide regulatory clarity and establish standards for handling virtual currencies within state financial programs. SB 822 specifically mandates the integration of virtual currency capabilities into the existing program framework to ensure SCO can effectively manage DFAs and meet its statutory obligations in returning unclaimed assets to rightful owners. In response to SB 822, SCO may seek information and/or vendor(s) to integrate virtual currency operations into the Program infrastructure.

4.0 Overview of Envisioned Example Approach to Custody

SCO, utilizing its substantial knowledge of unclaimed property administration and information technology (IT) systems, while acknowledging a less robust knowledge of virtual currency, has considered a variety of different, potential models for cryptocurrency custody. The overarching goal is to develop an efficient and seamless process for the transfer of unclaimed DFAs to the custodian; a functional interface between the custodian and the Program; automated authorization from the Program for the transfer of assets from the custodian to an approved claimant; and confirmation of successful claim payment from the custodian back to the Program. Essential to this initiative is the automation of processes to the fullest extent possible, incorporating electronic messaging.

SCO currently envisions a workflow as delineated below. *Note, however, that SCO encourages alternative approaches and will be agreeable to a different model that is more effective and cost-efficient.*

1. Holders of unclaimed DFAs will report to SCO with the underlying assets delivered to the State's account at the custodian. While holders will be provided with remittance instructions

prepared in conjunction with the custodian, the custodian may be required to assist holders having issues with DFA transfer to the custodian.

2. Utilizing the Report of Owners filed with SCO, the custodian will create subsidiary accounts or wallets for each individual owner/account reported. SCO will work with the custodian to transmit the report/owner detail electronically.

3. The custodian will perform an initial reconciliation of the State's DFA holdings to the aggregate owner subsidiary accounts/wallets created. The custodian will provide SCO with an interface to allow the owner subsidiary accounts/wallets to be viewed and identified by unique codes.

4. The Program will administer all claims and communications with claimants. When the Program approves a claim, the custodian will be notified with authorization and direction as to the transfer of assets within a wallet, be it transfer to a third party or liquidation. The State Treasurer's Office (STO) will assume responsibility for providing accurate direction and the custodian will assume responsibility for correctly and timely executing the directions. The custodian will notify the Program of any issues or delays that arise in "payment "of a claim.

5. The custodian will indicate when a claim has been discharged, and assets transferred out of the SCO's account/wallet. The Program will update its unclaimed property recordkeeping systems reflecting the claim as "paid."

6. The custodian will perform regular reconciliations of SCO's account/wallet to the aggregate subsidiary accounts/wallets created.

7. SCO may, from time to time, direct the liquidation of all assets in accounts/wallets which have remained unclaimed for a specified period of time following receipt by SCO [e.g., two (2) years]. The Program will identify the accounts/wallets to be liquidated, and the custodian will execute sales. The Program and the custodian will work together in reconciling the proceeds of sale to the closed subsidiary accounts/wallets.

8. The custodian will be responsible for all governmental tax compliance, including but not limited to the issuance of Form 1099s.

5.0 Looking Forward: Issue and Needs

1. **Secure Storage and Asset Protection**: Solutions must protect against theft, hacking, and loss. The solution should employ advanced security protocols, including multi-signature wallets, hardware security modules (HSMs), and secure cold storage.

2. **Regulatory Compliance**: Vendors must ensure compliance with state and federal laws, including unclaimed property statutes, financial regulations [e.g., Anti-Money Laundering (AML)/Know your Customer (KYC)], digital asset custody rules, and tax reporting.

3. **Operational Efficiency**: The custody solution should minimize the workload on state staff while providing intuitive tools for asset management and reporting. A provider should be able to assist in developing automated interfaces between the custodian's and the Program's IT planforms.

4. **Cost-Effectiveness**: Transparent pricing models with clear cost structures are required, ensuring the solution fits within budgetary constraints. Vendors should outline all potential fees, including hidden costs. Note: custodians will be permitted to deduct reasonable sales and blockchain fees from executed transactions.

5. **Scalability and Flexibility**: The solution must scale with the potential increase in wallet numbers, support a diverse range of digital assets, and have the capacity to support emerging cryptocurrencies and NFTs.

6. **Risk Mitigation**: Solutions must include insurance coverage for assets, protection against fraud, and a robust incident response plan in case of security breaches.

7. **Claimant Reunification**: This RFI explores various asset transfer options, including but not limited to — 1) transferring entire wallet control to claimants, 2) transferring assets directly to claimants' wallets, 3) transferring assets to claimants third party custodian, and 4) liquidation of assets with proceeds paid to the claimant.

6.0 RFI Responses

This RFI is not a Request for Proposals (RFP) or Invitation for Bids (IFB), nor will responses to this RFI be used as part of a vendor selection process or result in the award of a contract for such services. Any response to this RFI is for informational purposes only.

Respondents are not entitled to payment for either direct or indirect costs or charges because of submission of responses to this RFI.

SCO will review the responses to determine the feasibility of issuing a competitive solicitation in 2026. Any request for cost information is for budgetary purposes only. If necessary, SCO may ask to hold presentations with one (1) or more of the responding firms.

Firms that choose not to respond to this RFI are not precluded from participating in future solicitations, if issued. All materials submitted in response to this RFI become the property of SCO. Any portion of an RFI submission response that a vendor believes constitutes proprietary information entitled to an exception from disclosure pursuant to California State law, should be marked accordingly.

6.1 Firm Overview

6.1.1 Provide details about your company, including year established, jurisdiction where

domiciled, headquarters, and services offered. Highlight your experience with digital asset custody, particularly for governmental entities.

6.1.2 Include how your services differentiate from competitors.

6.1.3 Provide information regarding the financial stability of your company, including:

a. Financial reports or statements from the past three (3) years.

b. Identification of parent company, providing the same details for the parent as delineated in 6.1.1.

c. Information on investor backing, funding sources, or major clients that demonstrate financial stability. Identify any investor with a 5% or greater interest in the company.

d. Measures in place to ensure business continuity in case of financial challenges.

6.1.4 Who does the CISO report to? Who signs off on security investments and operational decisions?

6.2 Service Offerings

6.2.1 Describe the cryptocurrency and NFT custody solutions available for state-level management of unclaimed property. Include models such as institutional custody, cold storage, or other specialized services.

6.2.2 Outline your capacity to handle both cryptocurrency and NFT assets. Include any specialized features that cater to long-term asset holding.

6.2.3 Indicate whether a reappearing owner would be permitted to establish an account at your institution, or whether the reappearing owner would be required to transfer their virtual currency elsewhere.

6.2.4 Indicate whether your institution offers brokerage services or whether liquidations are handled by third parties. If third parties are utilized, explain how trades are executed.

6.3 Supported Digital Assets

6.3.1 Confirm support for the specific cryptocurrencies and NFTs identified in this RFI. Provide a schedule of all coins and other digital assets for which you currently provide custody. Describe how additional digital assets can be integrated as they are remitted or emerge.

6.3.2 Provide your process and the frequency for adding new asset types and blockchains to your custody solutions. Identify the number of new coins and other digital assets added during the preceding 12 months.

6.4 Security Measures

6.4.1 Detail security protocols, including cold storage, multi-signature wallets, Multi-Party Computation (MPC), Hardware Security Modules (HSMs), and protections against cyber and physical threats.

6.4.2 Outline encryption standards and any third-party security audits [e.g., System and Organization Controls 2 (SOC 2), International Organization for Standardization (ISO) 27001].

6.4.3 Provide information on your incident response plan, including how you handle breaches or attempted theft.

6.4.4 For NFTs, explain additional security considerations.

6.4.5 Provide an overview of your disaster recovery plan, including:

a. Time to recovery for services after a major incident.
b. Frequency of testing and updating the recovery plan.
c. Backup locations and procedures to ensure service continuity.
d. Resiliency measures (e.g., offsite replication, redundant data centers).

6.4.6 What measures are in place to secure your software/hardware supply chain, and how do you address vulnerabilities in third-party components?

6.4.7 What background checks, training programs, and access controls are implemented to minimize the risk of insider threats?

6.4.8 How do you monitor for and respond to signs of internal compromise?

6.5 Risk Management and Insurance

Outline your risk management policies. Describe insurance coverage, including incidents covered, policy limits, and whether NFTs are covered under the policy.

6.5.1 Provide details on any certifications, such as insurance certifications, that ensure protection of the assets.

6.5.2 What contractual assurances can be provided regarding liability for losses due to breach/incident?

6.5.3 What is the claims history against your insurance coverage?

6.6 Regulatory Compliance

6.6.1 Explain how your solution complies with relevant state and federal laws, including financial regulations, AML, and KYC requirements.

6.6.2 Provide information on licenses, registrations, or certifications related to cryptocurrency and NFT custody services.

6.6.3 Describe how you keep your solutions current with evolving regulations.

6.7 Cost Structure

6.7.1 Indicate your preferred pricing structure. If that structure is AUM, indicate whether you would consider a flat-fee or other model.

6.7.2 If your institution has a policy for a minimum annual fee, please identify such fee.

6.7.3 Provide a clear breakdown of your fee structure, including setup, custody, transaction, and additional service fees. Highlight any volume discounts or tiered pricing models. Explain the extent to which the fee is tied to transactions, and how transactional fees are charged. Indicate the availability of an annual fixed-price contract as opposed to fees based on AUM.

6.7.4 Please indicate whether in a custodial arrangement, sales and on-chain transactions are charged to the customer at cost, or whether there is a mark-up.

6.7.5 Include a detailed explanation of potential hidden fees or charges that could arise in different operational scenarios.

6.8 Technology and Integration

6.8.1 Describe your technology platform, including Application Programming Interface (API) access for integration with state systems. Provide details on how your system manages updates, maintenance, and security for sensitive client information.

6.8.2 Provide examples of successful integrations with governmental or institutional systems and share API documentation.

6.8.3 Describe your data management capabilities, including:

a. Data export options and supported formats [e.g., Comma Separated Values (CSV) , JavaScript Object Notation (JSON)].

b. Backup policies, including frequency, location, and procedures for data recovery.

c. Integration with third-party analytics platforms [e.g., Tableau, Power Business Intelligence (BI)] or built-in reporting and analytics features.

6.8.4 Provide details on how your platform integrates with existing financial systems or unclaimed property management systems used by the State of California.

a. List any systems or platforms your solution has previously integrated with [e.g., Enterprise Resource Planning (ERP) systems, accounting software].

6.8.5 Describe your experience in integrating with government systems or state/government-owned platforms.

6.9 Operational Aspects

6.9.1 Outline how you would go about establishing 4,000 subsidiary accounts/wallets (and up to 20,000 or more over time) where the state provides you with a feed of the underlying data for individual owners from unclaimed property reporting. Include tools for managing bulk transactions, tracking assets, and reducing staff workload.

6.9.2 Indicate what you believe to be the critical data elements which the State should request from holders of cryptocurrency when they report and remit unclaimed cryptocurrency.

6.9.3 Provide User Interface/User Experience (UI/UX) screenshots or mockups to demonstrate how your platform can be used by staff for account and asset management.

6.9.4 Detail the support you offer for training state employees and the operational support available post-implementation.

6.9.5 Detail your capacity to engage in development to facilitate interfaces between your operations and the IT platforms maintained by SCO.

6.10 Scalability

6.10.1 Explain how your solution scales to accommodate increasing numbers of wallets or assets over time. Identify any constraints or limitations on scalability.

6.10.2 Provide performance metrics from existing clients, such as the number of wallets managed, or the volume of transactions handled in high-scale scenarios.

6.11 Experiences and References

6.11.1 Provide case studies and references demonstrating your experience with similar institutions, particularly regarding custody of forfeited or unclaimed cryptocurrency or NFTs.

6.11.2 Highlight any challenges encountered while scaling your services and how they were overcome.

6.12 Compliance with Unclaimed Property Laws

6.12.1 Explain how your services comply with UPLs, including asset segregation, indefinite holding, and reporting obligations. Provide examples of how you've implemented similar legal frameworks with other clients.

6.13 Reporting and Transparency

6.13.1 Detail the types of reports available (e.g., asset holdings, audit logs), how frequently they are generated, and the customization options for regulatory or internal reporting.

6.13.2 Indicate the extent to which a customer can create and run custom reports.

6.13.3 Provide information on report formats [e.g., Portable Document Format (PDF), CSV, API data feeds] and real-time access options.

6.14 Asset Transfer and Claimant Reunification

6.14.1 Compare the options for asset transfer (transferring entire wallet control vs. transferring assets to claimants' wallets). Provide a recommendation based on security, legal compliance, and operational feasibility.

6.14.2 Explain how the Program would optimally provide you with actionable authorization/direction to transfer or liquidate coins for claimants, including authentication of the authorization/direction.

6.14.3 Describe the processes and security measures for transferring assets or wallets to rightful owners. Include possible processes for confirming/authenticating a transfer/payment instruction from the State.

6.15 Future Support and Development

6.15.1 Describe how you plan to support emerging cryptocurrencies and NFTs. Provide insight into your service enhancement roadmap and how client feedback influences future development.

6.15.2 Provide a timeline for introducing new features or support for emerging digital assets.

6.16 Legal and Contractual Considerations

6.16.1 Provide a copy of your standard service agreement. Highlight key contractual terms, including liability, dispute resolution, and third-party service provider policies.

a. Indicate the extent to which liability provisions are negotiable in view of the fact that the California State Controller's Office is bound by state laws that limit a waiver of state liability.

6.16.2 Indicate whether dispute resolution processes mandate arbitration and if so, whether this requirement can be/has been negotiated.

6.17 Optional Information

The Respondent may provide information to describe any additional or optional features that the Respondent can deliver within its solution or that would be helpful to the SCO in evaluating whether, and how, to contract with a private sector service provider for services described in this RFI.

7.0 Written Questions and Answers

1. Respondents may submit written questions for clarification of the content of this RFI via email to SCOBids@sco.ca.gov by the date and time specified in Section 11.0 Key Action Dates.

2. The subject line of the email should read, **RFI UPDRFI0125 Questions – Company Name**.

3. The Respondent must reference the section and page number about which they are inquiring.

4. Written Questions and Answers will be provided without identifying the submitter. SCO may paraphrase questions, at its sole discretion, for clarity.

5. Questions will not be answered by telephone.

6. Written Questions and Answers will be posted on Cal eProcure on or before the Written Questions & Answers Release date specified in Section 11.0 Key Action Dates.

8.0 Addenda or Changes to the RFI

SCO reserves the right to make changes to this RFI by posting addenda on the Cal eProcure portal prior to the RFI Response Submittal Due Date in RFI Section 11.0 Key Action Dates. It is the Respondent's responsibility to check for any posted addenda.

9.0 Response Submission

1. Submit an electronic copy of your response, via email, to SCOBids@sco.ca.gov. Responses should be received by the SCO no later than the time and date noted in Section 11.0, Key Action Dates.

2. Responses must reference the "***RFI UPDRFI0125 Digital Payment Services***" in the subject line of the email response submission.

3. Email Requirements:

    a. Respondents must ensure that emails do not exceed a file size of 20 megabytes.

    b. Respondents must ensure that emails do not contain scripts, executable files, password protections, or macros, which may make their emails undeliverable.

    c. Do not imbed links within the PDF—all documents must be contained within the PDF. SCO cannot access links to external sources. Submissions containing links to external sources will be rejected.

    d. If the email should exceed acceptable file size, the Respondent shall split the email into multiple emails to ensure delivery.

    e. Respondent submissions that are sent from unrecognized email servers may be blocked by SCO security filters and be flagged as spam, thereby rendering them not submitted.

    f. An automatic reply from SCOBids@sco.ca.gov confirms receipt of respondents' emails. A*utomatic replies only confirm receipt of emails and do not assess respondents' responsiveness to the RFI requirements in the email content or in any attachments therein.*

4. Response Content

    a. Cover Letter

    b. Executive Summary

        i. Narrative portions of submissions are limited to 8.5 x 11 inch paper, with 1-inch margins, single-spaced in Arial font size 12, and printable. Responses must not exceed 50 pages.

        ii. Acceptable formats include Microsoft Word (.doc), Microsoft Office Open Extensible Markup Language (XML) (.docx), Excel, and .pdf. Excel files must be in a sortable format.

iii. Non-narrative portions of submissions should be hosted by respondents for at least 90 days from response submission on a website managed by the Respondent. Any Uniform Resource Locators (URLs) and login credentials, as needed, should be provided. Submissions that require any form of additional authorization for access (e.g. demo sites) should accommodate access for a minimum of three (3) users.

c. Complete and submit Attachment A, Respondent Summary Page.

d. Complete and submit Attachment B, Certificate of Trade Secret.

e. Complete and submit Attachment C, Completed Response Checklist.

5. RFI Disposition

The information received shall be kept by SCO and made a part of a file or record, which will be open to public inspection.

If respondents believe any of its RFI response is exempt from disclosure under California Public Records Act, the Respondent shall complete and submit Attachment B, Certificate of Trade Secret and submit a fully redacted version of its information, clearly identified as the redacted version.

10.0 Presentations

At the sole discretion of the SCO, one (1) or more respondents may be selected to demonstrate the products and services relating to the information submitted in the RFI response. The presentations may be in person or virtual depending on contractors' preference and availability and will be no longer than 90 minutes.

11.0 Key Action Dates

The following key action details the activities, due dates and times that tasks should be completed during this RFI process. If the SCO finds it necessary to update any of the dates and times, it will issue an addendum to the RFI. All times listed below are in Pacific Standard Time (PST).

Key Action	Due Date	Time Due (PST)
Release of RFI	October 29, 2025	2:00 p.m.
Written Questions Submittal Due Date	**November 4, 2025**	**By 2:00 p.m.**
Written Questions and Answers Released	November 12, 2025	
RFI Response Submittal Due Date	**November 19, 2025**	**By 2:00 p.m.**
Optional Respondent Presentations	TBD	

ATTACHMENT A
Respondent Summary Page

By signing this page and submitting a response, the Respondent certifies:

1. The statements contained in the response are true and complete to the best of the Respondent's knowledge. The undersigned recognizes this is a public document and open to public inspection with the exception of items identified as a trade secret on Attachment B.

2. That any statements or representations contained in or attached to its response shall be used only for informational purposes and does not constitute a bid or a proposal in response to a formal solicitation.

Responding Firm:			
The contact person regarding this RFI is:			
Name & Title:			
Address:			
Phone Number:		Email:	
Cell Phone Number: (optional)	Fax Number:	Fax Number: (optional)	
The person authorized to bind the Respondent is:			
Name & Title:			
Address:			
Phone Number:		Email:	
Cell Phone Number: (optional)		Fax Number: (optional)	
Signature:			

ATTACHMENT B
Certificate of Trade Secret

_____ (Respondent), being first duly sworn under oath, and representing _____[Name] (hereafter "Respondent"), hereby deposes and swears or affirms under penalty of perjury that:

1. I have knowledge of the Request for Information, UPDRFI0125, and I have full authority to submit this affidavit and accept the responsibilities stated herein.

2. I am aware that the Respondent has submitted information, dated on or about [insert date] ("the Response"), to the State of California (State) in response to Request for Information, UPD-xxx, for Core Banking.

3. I have read and am familiar with the provisions of California's Public Records Act, California Government Code 7922.600. I understand that the information received as part of this RFI is a public record held by a public body and is subject to disclosure under the California Public Records Act unless specifically exempt from disclosure under that law.

4. I believe the information indicated is exempt from public disclosure (collectively, the "Exempt Information"), which is incorporated herein by this reference. It is my opinion that the Exempt Information constitutes "Trade Secrets" under either the California Public Records Act or the Uniform Trade Secrets Act as adopted in California because that information is either:

5. A formula, plan, pattern, process, tool, mechanism, compound, procedure, production data, or compilation of information that:

    a. Is not patented,
    b. Is known only to certain individuals within the Respondent's organization and that is used in a business the Respondent conducts,
    c. Has actual or potential commercial value, and
    d. Gives its user an opportunity to obtain a business advantage over competitors who do not know or use it.

    or

    e. Information, including a drawing, cost data, customer list, formula, pattern, compilation, program, device, method, technique or process that:
    f. Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and
    g. Is the subject of efforts by the Respondent that are reasonable under the circumstances to maintain its secrecy.

I understand that disclosure of the information referenced may depend on official or judicial determinations made in accordance with the Public Records Law.

Name & Title:	
Signature:	

ATTACHMENT C
Response Checklist

Please complete and return with your response.

Item	RFI Component
☐	Cover Letter
☐	Executive Summary
☐	Completed Attachment A, Respondent Summary Page
☐	Completed Attachment B, Certificate of Trade Secret
☐	Completed Attachment C, Response Checklist

Check the box(es) to indicate the portions of the RFI you are responding to.

Check		RFI Component	Documents (Document Title or URL)
6.1 Firm Overview			
☐	6.1.1	Company Details	
☐	6.1.2	Unique Services	
☐	6.1.3	Financial Stability	
☐	6.1.4	Information Security Structure	
6.2 Service Offerings			
☐	6.2.1	Custodial Solutions	
☐	6.2.2	Asset Holding Capacity	
☐	6.2.3	Owner Account Protocol	
☐	6.2.4	Brokerage and Liquidation	
6.3 Supported Digital Assets			

☐	6.3.1	Current Digital Asset Support	
☐	6.3.2	Increase Assets	
6.4 Security Measures			
☐	6.4.1	Protocols	
☐	6.4.2	Encryption	
☐	6.4.3	Incident Response	
☐	6.4.4	Security Considerations	
☐	6.4.5	Disaster Recovery	
☐	6.4.6	Third-Party Vulnerabilities	
☐	6.4.7	Access Controls	
☐	6.4.8	Internal Compromise	
6.5 Risk Management and Insurance			
☐	6.5.1	Insurance Certificates	
☐	6.5.2	Loss Liability – Breach/incident	
☐	6.5.3	Insurance Claim History	
6.6 Regulatory Compliance			
☐	6.6.1	Compliance with Laws and Regulations	
☐	6.6.2	Licenses, Registration, Certifications	
☐	6.6.3	Evolving Regulations	
6.7 Cost Structure			
☐	6.7.1	Pricing Structure	
☐	6.7.2	Minimum Fee	

☐	6.7.3	Fee Structure	
☐	6.7.4	Transaction Costs	
☐	6.7.5	Unique Scenarios	
6.8 Technology and Integration			
☐	6.8.1	Application Programming Interface	
☐	6.8.2	Government Integrations	
☐	6.8.3	Data Management Capabilities	
☐	6.8.4	Platform Integration	
☐	6.8.5	Government Integration	
6.9 Operational Aspects			
☐	6.9.1	Establishing Subsidiaries	
☐	6.9.2	Critical Data Elements	
☐	6.9.3	User Interface/User Experience	
☐	6.9.4	Operational/Training Support	
☐	6.9.5	Development Engagement	
6.10 Scalability			
☐	6.10.1	Case Studies	
☐	6.10.2	Performance Metrics	
6.11 Experiences and References			
☐	6.11.1	Case Studies	
☐	6.11.2	Challenges	
6.12 Compliance with Unclaimed Property Laws			

☐	6.12.1	Legal Framework Implementation	
6.13 Reporting and Transparency			
☐	6.13.1	Reports	
☐	6.13.2	User Experience	
☐	6.13.3	Formats and Access	
6.14 Asset Transfer and Claimant Reunification			
☐	6.14.1	Asset Transfer Recommendations	
☐	6.14.2	Actionable Authentication	
☐	6.14.3	Asset Transfer Authentication	
6.15 Future Support and Development			
☐	6.15.1	Roadmap	
☐	6.15.2	Timeline	
6.16 Legal and Contractual Considerations			
☐	6.16.1	Standard Service Agreement	
☐	6.16.2	Dispute Resolution	
6.17 Optional Information			
☐	6.17.1	Additional or Optional Features	