THE CRYPTO RECOVERY PLAYBOOK

A Comprehensive Guide for Legal Professionals

Managing Partner: Ohoon Kwon (ohkwon@chakwon.com)

TABLE OF CONTENTS

INTRODUCTION

Cryptocurrency theft and fraud continue to present some of the most challenging asset recovery scenarios facing legal practitioners today. This playbook provides a comprehensive framework for attorneys, forensic investigators, and compliance professionals responding to crypto-asset theft or loss.

The methodologies outlined here have been developed and field-tested through dozens of real-world recovery actions across multiple jurisdictions, asset classes, and attack

vectors. They represent the accumulated institutional knowledge of Cha & Kwon's crypto-asset practice since 2018.

While each case presents unique attributes, this framework offers a structured approach to maximize recovery probability and minimize the time between asset loss and potential recovery or freezing.

How to Use This Playbook:

This document is designed to be both a reference guide and an operational manual. Sections are modular and cross-referenced for rapid deployment during active incidents.

BEFORE THE CRISIS: PREPARATION

Successful crypto-asset recovery begins long before any assets are stolen. This section outlines essential preparation steps for legal teams and their clients.

1. Asset Mapping and Documentation

Best Practices for Clients:

- Maintain a secure, off-chain record of all wallet addresses and associated custody arrangements
- Document administrative access controls to exchange accounts, hot wallets, and cold storage solutions
- Establish baseline transaction patterns to identify anomalies quickly
- Implement regular backup procedures for private key material and seed phrases
- Regularly audit and test recovery mechanisms

2. Relationship Development

Pre-establish relationships with:

- Local law enforcement with cyber expertise
- Regulatory authorities in relevant jurisdictions
- Key exchanges and VASPs for expedited subpoena/disclosure processes
- Forensic blockchain analysis firms

- Technical cryptocurrency experts with court testimony experience
- Local counsel in common crypto-friendly jurisdictions

3. Legal Preparations

Prepare template documents for rapid deployment:

- Ex parte freeze applications for major jurisdictions
- Norwich Pharmacal/third-party disclosure applications
- Emergency arbitration requests
- Criminal referral packages
- Pre-drafted affidavits covering blockchain technology explanations

4. Chain-Specific Considerations

Technical preparation for major chains:

Bitcoin:

- Configure real-time withdrawal alerts from material addresses
- Establish relationships with major mining pools for potential transaction intervention
- Document coinbase-to-address maturity for relevant holdings (temporal traceability)

Ethereum:

- Document smart contract dependencies and admin keys
- Maintain current list of major wrapped asset contracts and bridge facilities
- Establish alert systems for material gas spikes indicating potential MEV exploitation

Stablecoins:

- Document chain-specific blacklist/freeze capabilities of major issuers
- Maintain direct legal escalation contacts with major stablecoin issuers
- Prepare declarations explaining stablecoin mechanisms for non-technical courts

---

THE SIX-STEP RECOVERY FRAMEWORK

STEP 1: RAPID RESPONSE PROTOCOL

Objective: Secure freezing orders and preservation notices within 24 hours of theft discovery.

Initial Assessment (First 60 Minutes)

Critical Questions:

- When was the theft discovered and when did it likely occur?
- What is the estimated amount and type of assets taken?
- Have the assets moved from the initial theft destination?
- What security mechanisms were compromised?
- Are private keys or authentication credentials still at risk?
- Are insider threats a possibility?

Documentation Requirements:

- Screenshots of relevant transactions and wallet interfaces
- Access logs from relevant time periods
- Any correspondence with potential attackers
- Transaction IDs and wallet addresses involved
- Internal security assessment

Immediate Technical Actions

1. **Blockchain Monitoring Set-up:**
    - Implement real-time monitoring of identified addresses
    - Deploy automated alerts for any further movement of funds
    - Engage forensic blockchain analysts for initial trace report
2. **Transaction Pattern Analysis:**

- Identify if theft matches known attack signatures
- Determine if exchange cashout has begun or appears imminent
- Assess velocity of fund movement (rapid splitting vs. dormant holding)
- Evaluate cross-chain bridge usage

3. **Immediate Technical Preservation:**
    - Mirror affected systems and create forensic images
    - Preserve all logs with chain-of-custody documentation
    - Secure backup of all transaction data and wallet interactions

Priority Legal Actions

1. **Freezing Order Preparation:**
    - Jurisdiction selection based on:
        - Location of known exchanges involved
        - Domicile of theft victim
        - Location of suspected perpetrators
        - Legal systems with pre-existing cryptocurrency jurisprudence
    - Order scope determination:
        - "World-wide" vs. jurisdiction-specific language requirements
        - Asset class specification and identification metrics
        - Duration and renewal mechanisms
        - Affected intermediary notification requirements
2. **Critical Filings (24-Hour Window):**
    - Ex parte freezing applications in priority jurisdictions
    - Mareva injunctions where appropriate
    - Temporary restraining orders with asset freeze provisions
    - Emergency arbitration notices if relevant contract provisions exist

- Police reports in relevant jurisdictions (even if no immediate action expected)

STEP 2: EVIDENCE PRESERVATION

Objective: Secure comprehensive technical and financial evidence before degradation or intentional destruction can occur.

Technical Evidence Preservation

1. **Full-Node Snapshots:**
    - Secure blockchain nodes relevant to the affected chains
    - Document hash values and timestamp node data
    - Implement forensic verification of snapshot integrity
    - Maintain chain-of-custody documentation for potential court proceedings
2. **Chain-State Exports:**
    - Generate merkle-proof timestamps of relevant addresses
    - Document balance states immediately pre- and post-incident
    - Preserve smart contract states where applicable
    - Create validator-signed attestations where possible
3. **Security System Logs:**
    - Preserve authentication logs with timestamp verification
    - Secure API access records with IP metadata
    - Document 2FA/MFA state changes and authentication attempts
    - Preserve SIEM alerts and security tool outputs
4. **Exchange Interaction Evidence:**
    - Document account access patterns
    - Preserve withdrawal authorization evidence
    - Secure KYC/AML verification history
    - Screenshot account status and balance information

Forensic Documentation Standards

Ensuring Admissibility:

- Maintain unbroken chain of custody documentation
- Use write-once media where possible for storage
- Implement dual-control procedures for evidence handling
- Generate cryptographic timestamps of evidence collection
- Secure third-party attestation of critical evidence where possible

Documentation Requirements:

- Who: Identity of evidence collector and witnesses
- What: Precise description of evidence collected
- When: Date and time of collection (with timezone specification)
- Where: Physical or digital location where evidence was collected
- How: Technical methods used to collect and preserve evidence
- Why: Purpose of collection and relevance to the case

Temporal Evidence Considerations:

- Standardize all timestamps to UTC for consistency
- Document timezone offsets in local records
- Establish chronology of events with confidence intervals
- Cross-reference timestamps from multiple sources to establish reliability

Evidence Storage Security

Best Practices:

- Implement air-gapped storage for critical evidence
- Create multiple encrypted backups with distributed key custody
- Establish role-based access controls for evidence review
- Implement tamper-evident storage mechanisms

- Document every access to evidence with purpose and authorization

Cloud Storage Considerations:

- Select jurisdictionally appropriate storage locations
- Implement enhanced encryption beyond provider defaults
- Establish legal compliance with chain-of-custody requirements
- Document data sovereignty implications of storage choices

Legal Holds and Preservation Notices

Internal Preservation Protocol:

- Issue formal legal hold notices to all relevant personnel
- Document receipt and acknowledgment of preservation obligations
- Conduct preservation interviews with key witnesses
- Create evidence preservation logs with custodian information

External Preservation Notices:

- Send formal preservation requests to relevant exchanges and VASPs
- Issue preservation demands to cloud service providers
- Notify Internet Service Providers of potential log requirements
- Contact domain registrars for relevant phishing or fraud domains

STEP 3: PARALLEL LEGAL STRATEGIES

Objective: Pursue multiple legal avenues simultaneously to maximize recovery potential and apply pressure from different angles.

Strategy Matrix

Legal Avenue	***Primary Purpose***	***Timeline***	***Key Advantages***	***Limitations***
Civil Litigation	Asset recovery & damages	Immediate filing	Speed; direct control	Expensive; enforcement challenges

Criminal Referral	Asset seizure & prosecution	After evidence gathering	State resources; cross-border tools	Limited control; variable priority
Regulatory Action	Systemic pressure & assistance	After initial assessment	Industry-wide leverage; VASP pressure	Broader focus; slower response
Arbitration	Contractual recovery	Per agreement terms	Privacy; specialized tribunal	Limited to contract parties

Civil Strategy Components

Immediate Actions:

- File for preliminary injunctions and freezing orders
- Seek disclosure orders against third parties
- Implement service via alternative means where necessary
- Consider provisional liquidator appointment where shell companies involved

Jurisdictional Strategy:

- Primary jurisdiction: Location with strongest connection to assets or parties
- Secondary jurisdictions: Key off-ramp locations and exchange domiciles
- Enforcement jurisdictions: Where assets are likely to materialize in recoverable form

Common Law Advantage Points:

- Utilize proprietary tracing principles unique to common law systems
- Implement constructive trust arguments for commingled funds
- Deploy unjust enrichment claims as fallback positions
- Consider equitable remedies including account of profits

Civil Law Considerations:

- Leverage data protection regulations for information disclosure

- Utilize provisional measures available under civil codes
- Consider specific performance remedies where available
- Implement moral damages claims where relevant

Criminal Strategy Components

Law Enforcement Engagement:

- Identify optimal jurisdictions for criminal referral
- Prepare comprehensive criminal complainant packages
- Develop relationships with specialized cyber units
- Provide technical education for assigned investigators

Strategic Considerations:

- Balance information sharing with confidentiality needs
- Coordinate civil and criminal timelines to avoid conflicts
- Prepare for potential asset seizure and forfeiture proceedings
- Develop victim restitution strategy for post-conviction phase

Cryptocurrency-Specific Criminal Provisions:

- Identify jurisdictions with specific cryptocurrency theft statutes
- Evaluate computer crime provisions that explicitly cover wallet credentials
- Consider money laundering predicate offenses relevant to crypto
- Assess anti-fraud provisions applicable to smart contract manipulation

Evidence Package for Law Enforcement:

- Technical explanation of theft mechanism
- Blockchain transaction analysis in non-technical format
- Visualization of fund flow with key decision points
- Suspect identification information (if available)
- Financial impact statement

- Chain of custody documentation for all evidence

Regulatory Strategy Components

Key Regulatory Bodies by Jurisdiction:

Jurisdiction	*Primary Regulator*	*Focus Area*	*Enforcement Tools*
United States	FinCEN / SEC / CFTC	AML / Securities / Derivatives	Examinations; Enforcement actions
European Union	National FIUs / ESMA	AML / Market integrity	Administrative penalties; Operational restrictions
Singapore	MAS	Comprehensive	License revocation; Financial penalties
UAE	VARA / FSRA	Virtual assets / Financial services	Regulatory directives; Administrative actions
UK	FCA / NCA	Financial services / Crime	Warning notices; Restricted activity orders

Engagement Strategy:

- File suspicious activity reports in relevant jurisdictions
- Provide technical briefings to specialist regulatory teams
- Request exchange compliance reviews where appropriate
- Seek regulatory assistance letters for cross-border matters

Regulatory Pressure Points:

- VASP licensing conditions and requirements
- Travel Rule compliance obligations
- Market manipulation prohibitions
- AML/CTF compliance frameworks

STEP 4: TARGETING CHOKE POINTS

Objective: Identify and apply strategic pressure to key points where stolen crypto-assets must pass through centralized control or conversion.

Exchange Targeting Strategy

Identification Process:

- Monitor stolen funds for movement toward known exchange deposit addresses
- Analyze gas fees and withdrawal patterns for exchange footprint
- Identify exchange-specific token patterns in transaction flow
- Monitor mempool for pending transactions to exchange wallets

Exchange Types and Approach Matrix:

Exchange Type	*Jurisdiction Example*	*Approach Strategy*	*Documentation Needs*
Tier 1 Regulated	Coinbase (US)	Formal legal process	Court order; SAR filing
Tier 2 Regulated	Regional exchanges	Direct compliance contact + legal	Freeze declaration; Chain analysis
Tier 3 Limited Regulation	Emerging market exchanges	Heightened pressure; multiple channels	Expanded evidence package; Media strategy
Non-Compliant	Jurisdiction-evading exchanges	Regulatory escalation; indirect pressure	Enforcement referrals; Public exposure

Expedited Process Template:

1. Direct compliance team contact
2. Simultaneous submission of:
    - Formal freeze request letter
    - Evidence package with transaction tracing
    - Court orders (if obtained)
    - Law enforcement contact information
3. Escalation to legal counsel after 4 hours without response
4. Regulatory notification after 12 hours without response

OTC Desk Strategy

Identification Markers:

- Large, round-number transactions
- Unusual token pairings or conversion patterns

- Direct wallet-to-wallet transfers with value negotiation patterns
- Known OTC desk wallet interactions

Engagement Approach:

- Direct outreach to compliance teams with evidence package
- Industry association pressure where applicable
- Implementation of "proceed of crime" notifications
- Strategic use of international financial intelligence units

Documentation Requirements:

- Comprehensive transaction flow analysis
- Clear demonstration of illicit source
- Contact chain documentation
- Timestamped communication records

Bridge and Cross-Chain Choke Points

Key Bridge Protocols and Approaches:

Bridge	*Chains Connected*	*Freezing Capability*	*Contact Strategy*
Portal Bridge	Solana-Ethereum	Limited - multisig governance	DAO governance proposal + guardian outreach
Polygon Bridge	Ethereum-Polygon	Yes - via governance	Direct team contact + validator pressure
Multichain	Multiple	Protocol dependent	Security team + backchannel validator contact
Wormhole	Multiple	Guardian oversight	Direct security team outreach

Bridge Intervention Strategy:

1. Identify involved bridges from transaction flow
2. Contact bridge development team and security contacts
3. Prepare technical package specific to bridge architecture
4. Leverage community governance where applicable
5. Implement validator/node operator outreach in parallel

STEP 5: ESTABLISHING A FUSION CELL

Objective: Create an integrated, multidisciplinary team with clear communication channels, defined responsibilities, and unified strategy to maximize recovery effectiveness.

Core Team Composition

Required Roles:

Role	*Responsibility*	*Key Skills*	*Available Hours*
Lead Counsel	Legal strategy; client interface	Asset recovery expertise; litigation management	24/7 during critical phase
Forensic Analyst	Transaction tracing; technical analysis	Blockchain expertise; investigative skills	24/7 during critical phase
Local Counsel (per jurisdiction)	Jurisdiction-specific filings; court appearances	Local procedural knowledge; crypto experience	Business hours + emergency
Technical Expert	Blockchain mechanics; expert testimony	Deep protocol knowledge; communication skills	On-call basis
Client Representative	Decision authority; resource allocation	Organizational authority; industry knowledge	Regular briefing schedule
PR/Communications (if public)	Media management; narrative control	Crisis communication; industry connections	As needed

Extended Team as Needed:

- Law enforcement liaison
- Regulatory specialists
- Exchange relationship managers
- Blockchain development consultants

- Specialized investigators
- Data privacy counsel

Operational Structure

Command and Control:

- Designate single decision authority with clear escalation paths
- Implement formal approval process for critical decisions
- Establish communication protocols and secure channels
- Define reporting cadence and format standards

Information Management:

- Centralize evidence and strategy documentation in secure repository
- Implement need-to-know protocols for sensitive information
- Create standardized briefing templates for consistency
- Maintain real-time case management dashboard

Communication Framework:

- Primary: End-to-end encrypted messaging platform
- Secondary: Encrypted email with PGP verification
- Emergency: Pre-established call protocol with verification procedures
- Client Updates: Scheduled secure briefings with standardized format

Operational Tempo:

- Initial Phase (0-72 hours): Continuous operation with 8-hour rotation shifts
- Active Phase (72+ hours): 12-hour operational periods with defined handovers
- Monitoring Phase: Scheduled check-ins with alert-based escalation

Cross-Border Coordination

Jurisdictional Alignment:

- Harmonize legal strategy across multiple jurisdictions

- Implement conflicting order risk assessment
- Develop filing coordination timeline
- Establish unified evidence standards compliant with all relevant jurisdictions

Time Zone Management:

- Designate primary time reference (typically UTC)
- Maintain 24-hour coverage during critical phases
- Schedule key decision points to maximize availability
- Document timezone considerations in all filings

Language and Cultural Considerations:

- Utilize certified translation services for all formal documents
- Account for local procedural customs and expectations
- Develop jurisdiction-specific relationship approaches
- Maintain awareness of cultural factors in negotiation strategy

Resource Allocation Framework

Budget Tiers Based on Asset Value:

Asset Value Range	*Recommended Budget*	*Resource Allocation Focus*
<$100,000	15-25% of asset value	Focused exchange outreach; limited legal action
$100,000-$1M	10-15% of asset value	Targeted legal in 1-2 jurisdictions; forensic tracing
$1M-$10M	5-10% of asset value	Multi-jurisdiction approach; full fusion cell
$10M+	2-5% of asset value	Comprehensive global strategy; extended team

Cost-Benefit Decision Framework:

- Establish clear recovery probability metrics
- Develop stage-gate approach with continue/abandon criteria
- Implement regular strategy reassessment protocol
- Document risk/reward calculations for major expenditures

STEP 6: POST-SEIZURE MONITORING

Objective: Maintain vigilance after initial freezing or recovery to prevent circumvention attempts, secondary attacks, and ensure complete asset security.

Ongoing Monitoring Protocol

Technical Monitoring:

- Maintain blockchain surveillance of known addresses
- Implement alerts for related address activity
- Monitor for fork-based replay attempts
- Track wrapped asset versions of frozen tokens
- Analyze mempool for pending transactions

- Monitor validator/miner activity for unusual patterns

Monitoring Duration Guidelines:

Asset Type	*Minimum Monitoring Period*	*Alert Triggers*	*Review Cadence*
Bitcoin	6 months	Address activity; UTXO movement	Daily for 30 days, then weekly
Ethereum/EVM	3 months	Contract interaction; Gas spike	Daily for 30 days, then weekly
Stablecoins	12 months	Blacklist circumvention; New issuance	Weekly for 90 days, then monthly
Privacy Coins	24 months	Exchange deposits; Mixing activity	Weekly ongoing

Monitoring Tool Configuration:

- Set up dedicated wallet watchers for all identified addresses
- Implement webhook alerts for real-time notification
- Configure blockchain node alerts for relevant transactions
- Establish dark web monitoring for address discussions

Circumvention Attack Vectors

Common Evasion Techniques and Countermeasures:

Evasion Technique	*Detection Method*	*Countermeasure*
"Dusting" Attempts	Small value transfer monitoring	Supplemental freezing orders with "tainted proceeds" language
Alternative Fork Usage	Cross-chain analytics	Expanded freeze orders covering fork-based assets
Wrapped Token Conversion	Bridge monitoring	Issuer notifications; secondary freeze actions
"Good Faith Purchaser" Claims	Transaction pattern analysis	Pre-emptive notification to major exchanges
DeFi Liquidity Pool Hiding	Protocol-specific monitoring	Pool-based tracing; governance outreach
Hardware Wallet Migration	Address clustering analysis	Expanded freeze orders; law enforcement notification

Response Protocols:

- Implement countermeasure decision trees for common scenarios
- Maintain rapid response team for circumvention attempts
- Develop template supplemental filings for emerging techniques
- Establish accelerated court access for urgent modifications

Legal Process Maintenance

Order Renewal Strategy:

- Calendar all order expiration dates with advance warnings
- Prepare extension documentation in standard format
- Document ongoing risk of dissipation with current evidence

- Maintain relationship with court personnel for procedural guidance

Compliance Documentation:

- Maintain detailed records of compliance with all order terms
- Document all notification attempts and responses
- Preserve chain of evidence for all post-order activities
- Prepare regular status reports in court-ready format

Final Recovery Process

Asset Return Mechanisms:

Asset Type	*Return Method*	*Security Considerations*	*Documentation Requirements*
Bitcoin	Staged return to new secure wallet	Multi-signature controls; Witness process	Transaction verification; Receipt confirmation
Ethereum/EVM	Smart contract release mechanism	Audited contract; Phased release	On-chain verification; Technical certification
Stablecoins	VASP-assisted return or conversion	Approved channel verification; AML checks	Compliance certifications; Receipt validation
Exchange-Held	Direct account transfer or wire	Settlement agreement; Release confirmation	Transfer confirmation; Legal acknowledgment

Verification Standards:

- Multi-party validation of all recovery transactions
- Independent technical verification of asset authenticity
- Formal receipt and release documentation
- Final transaction reconciliation with original loss

JURISDICTIONAL CONSIDERATIONS

United States

Key Venues:

- Southern District of New York: Preferred for exchange-related matters
- Northern District of California: Tech-focused with blockchain familiarity
- Eastern District of Virginia: Speed advantages for emergency relief

Procedural Advantages:

- Asset freeze via TRO available ex parte with proper showing
- Nationwide effect of federal court orders
- Broad third-party discovery via Rule 45 subpoenas
- Robust contempt powers for non-compliance

Cryptocurrency Jurisprudence:

- SEC v. Telegram Group (S.D.N.Y. 2020): Established jurisdiction over token offerings
- United States v. Gratkowski (5th Cir. 2020): Limited privacy expectation in blockchain records
- Kleiman v. Wright (S.D. Fla. 2021): Recognition of bitcoin as property with legal protections

Strategic Approach:

- Emphasize securities aspects where applicable to leverage SEC involvement
- Utilize wire fraud provisions for expansive jurisdiction
- Consider parallel civil forfeiture proceedings where law enforcement engaged
- Leverage MLAT processes for international evidence gathering

United Kingdom

Key Venues:

- Business and Property Courts (London): Primary venue for complex crypto cases
- Commercial Court: High-value international disputes
- Chancery Division: Proprietary claims and tracing

Procedural Advantages:

- Worldwide freezing orders (WFO) with extraterritorial effect
- Robust Bankers Trust disclosure jurisdiction
- Norwich Pharmacal third-party disclosure

- Established cryptocurrency jurisprudence

Cryptocurrency Jurisprudence:

- AA v. Persons Unknown [2019] EWHC 3556 (Comm): Bitcoin recognized as property
- Ion Science Ltd v. Persons Unknown (2020): Jurisdiction over crypto fraud established
- Fetch.ai Ltd v. Persons Unknown [2021] EWHC 2254 (Comm): Framework for exchange-based recovery

Strategic Approach:

- Focus on proprietary tracing principles for commingled funds
- Utilize robust disclosure mechanisms against VASPs
- Seek passport recognition of orders in key jurisdictions
- Implement contempt enforcement for international compliance

Singapore

Key Venues:

- Singapore International Commercial Court: Complex international cases
- High Court: Commercial List for expedited matters

Procedural Advantages:

- Recognition as leading crypto jurisdiction in Southeast Asia
- Established proprietary injunctions for cryptocurrency
- Expedited disclosure processes for digital assets
- Strategic location for Asian exchange enforcement

Cryptocurrency Jurisprudence:

- B2C2 Ltd v. Quoine Pte Ltd [2019] SGHC(I) 03: Smart contract enforcement
- CLM v. CLN [2022] SGHC 46: Proprietary injunctions for cryptocurrency
- Bybit Fintech Limited [2023]: Regulatory framework application

Strategic Approach:

- Leverage Singapore's position as financial hub for regional enforcement
- Utilize specific crypto-asset focused procedures
- Implement exchange relationship network for informal pressure
- Focus on technical understanding of Singapore courts

European Union

Key Jurisdictions:

- France: Active enforcement, AMF engagement
- Germany: BaFin recognition of crypto-assets
- Malta: Cryptocurrency legislative framework

Procedural Considerations:

- MiCA regulation implementation timeline
- Jurisdiction-specific freezing mechanisms
- Data protection implications of blockchain tracing
- Civil law approach to proprietary remedies

Cryptocurrency Jurisprudence:

- Varies significantly by member state
- European Court of Justice: Hedqvist case on VAT treatment

Strategic Approach:

- Target jurisdiction selection based on asset location
- Utilize EU-wide enforcement where possible
- Implement data protection leveraged disclosure requests
- Focus on consumer protection aspects where relevant

UAE/DIFC/ADGM

Key Venues:

- Dubai International Financial Centre (DIFC) Courts
- Abu Dhabi Global Market (ADGM) Courts
- Onshore UAE Federal Courts

Procedural Advantages:

- DIFC/ADGM: Common law systems with strong freezing remedies
- Onshore UAE: Expedited processes for financial crimes
- Emerging crypto regulation with enforcement mechanisms

Strategic Considerations:

- Increasing importance as crypto industry hub
- Relationship-dependent enforcement efficiency
- Varying technical sophistication by forum
- Critical for regional exchange/OTC coverage

Hong Kong

Key Venues:

- High Court of Hong Kong: Commercial List

Procedural Advantages:

- Strong common law freezing and disclosure remedies
- Strategic for Asian exchange enforcement
- Developed cryptocurrency jurisprudence
- Gateway to Chinese-based recovery

Cryptocurrency Jurisprudence:

- Yan Yu Ying v. Leung Wing Hei [2022] HKCFI 1660: Cryptocurrency account of profits
- Nico Constantijn Antonius Samara v. Stive Jean Paul Dan [2022] HKCFI 1254: Freezing injunctions

Strategic Approach:

- Utilize for regional exchange coverage
- Implement in parallel with Singapore strategy
- Focus on proprietary remedies and disclosure
- Leverage for Chinese exchange pressure

TECHNICAL TOOLKIT GUIDE

In-House vs. External Services:

- In-house deployment: Control and speed advantages
- External service engagement: Expertise and testimony credibility
- Hybrid approach: Initial external analysis with in-house follow-up

Output Standardization:

- Evidence-grade report formatting
- Courtroom-ready visualizations
- Expert declaration templates
- Technical appendix frameworks

Wallet and Key Management

Secure Key Custody Standards:

- Multi-signature quorum requirements (minimum 2-of-3)
- Hardware security module integration
- Air-gapped signing procedures
- Deadman switch contingencies

Recovery Fund Security:

- Segregated recovery wallets with enhanced security
- Multi-party authorization for any movement
- Transaction signing ceremony documentation
- Independent verification of recovery addresses

Exchange Account Security:

- Whitelisted withdrawal addresses only
- IP restriction implementations

- Advanced authentication requirements
- Transaction limit controls

Technical Evidence Collection

On-Chain Data Collection:

- Full node verification procedure
- Transaction hash documentation standards
- Merkle path verification requirements
- Block explorer screenshot protocol

Exchange API Evidence:

- Rate limit considerations
- Authentication preservation
- Response validation
- Timestamp correlation

Smart Contract Analysis:

- Source code preservation
- Decompiled bytecode documentation
- Function signature verification
- State change logging

Blockchain Specific Approaches

Bitcoin Considerations:

- UTXO tracking methodology
- Coinbase maturity evaluations
- Fee analysis for urgency determination
- Input/output heuristics

Ethereum Considerations:

- Smart contract interaction tracing
- Gas price analysis for priority indicators
- Internal transaction documentation
- Event log preservation

Cross-Chain Considerations:

- Bridge transaction correlation
- Wrapped asset tracking
- Liquidity pool analysis
- Atomic swap identification

COMMON PITFALLS AND HOW TO AVOID THEM

Pitfall 1: Delayed Response Timeline

Common Manifestations:

- Internal approval processes delaying legal action
- Sequential rather than parallel response tracks
- Excessive evidence gathering before initial freezing attempts
- Technical analysis paralysis

Prevention Strategy:

- Implement pre-approved emergency response protocols
- Establish clear authorization thresholds and delegations
- Develop template documents for immediate deployment
- Create tiered evidence standards for initial vs. follow-up actions

Remediation If Encountered:

- Shift to preservation-focused strategy
- Implement broad-based exchange alerts

- Concentrate on remaining choke points
- Consider voluntary return negotiation

Pitfall 2: Jurisdictional Misalignment

Common Manifestations:

- Pursuing orders in jurisdictions without effective enforcement capability
- Failing to cover all major exchange jurisdictions
- Conflicting orders across different legal systems
- Inefficient allocation of legal resources

Prevention Strategy:

- Develop asset flow prediction models for jurisdiction targeting
- Maintain current exchange jurisdiction database
- Implement coordination protocol for multi-jurisdiction actions
- Prioritize jurisdictions by enforcement effectiveness not legal elegance

Remediation If Encountered:

- Reassess jurisdiction strategy based on current asset location
- Implement mutual recognition applications where available
- Focus resources on highest-probability recovery jurisdictions
- Consider alternative legal theories in key jurisdictions

Pitfall 3: Technical Evidence Inadequacy

Common Manifestations:

- Chain of custody breaks in blockchain evidence
- Insufficient technical explanation for non-specialist courts
- Inadmissible screenshots or unverified explorer data
- Missing transaction hash verification

Prevention Strategy:

- Implement forensic-grade evidence collection protocols
- Develop court-ready explanation templates for blockchain mechanics
- Utilize qualified expert declarations for technical validation
- Maintain original format data with verification hashes

Remediation If Encountered:

- Obtain independent verification of existing evidence
- Develop supplemental technical declarations
- Provide enhanced visual aids for judicial understanding
- Consider court-appointed expert processes

Pitfall 4: Exchange Relationship Failures

Common Manifestations:

- Over-reliance on formal legal process for non-cooperative exchanges
- Insufficient detail in initial freeze requests
- Failure to leverage regulatory relationships for pressure
- Inconsistent follow-up protocol

Prevention Strategy:

- Maintain current exchange contact database with escalation paths
- Develop relationship-based channels before incidents occur
- Create exchange-specific package templates
- Implement systematic follow-up protocol with escalation triggers

Remediation If Encountered:

- Activate secondary pressure channels (regulators, banking partners)
- Enhance evidence package with additional detail
- Implement public transparency strategy where appropriate
- Consider legal action against exchange itself

Pitfall 5: Resource Misallocation

Common Manifestations:

- Excessive resources dedicated to low-probability recovery paths
- Insufficient investment in high-value jurisdiction actions
- Premature abandonment of viable recovery channels
- Failure to adjust strategy as asset movement occurs

Prevention Strategy:

- Implement stage-gate approach with clear success metrics
- Develop probability-adjusted resource allocation model
- Require regular strategy reassessment at defined intervals
- Maintain flexible resource deployment capability

Remediation If Encountered:

- Conduct comprehensive cost-benefit reassessment
- Reallocate resources to highest-probability remaining channels
- Consider partial recovery negotiation where appropriate
- Implement lessons-learned protocol for future incidents

For additional information or to schedule a consultation regarding crypto-asset recovery planning or active incidents, please contact:

Cha & Kwon Law Offices
Crypto-Asset Recovery Practice
Email: contact@chakwon.com

legal advice.

Document version 1.0