#1

OCT 2025

lexcrypta

NEWSLETTER

Who is Lexcrypta?

Lexcrypta helps lawyers and accountants verify, trace, and secure digital assets with confidence. From redacted bank statements to full-scale crypto tracing, our secure, compliant workflow delivers clear results—fast.

www.lexcrypta.com

+1 313 799 3236

Quick Snapshot

S**elf-Custodied Wallet** These are wallets (e.g., MetaMask, Ledger, Trust Wallet) where the user holds the private keys. No exchange or third party controls access—making legal recovery difficult without cooperation or forensic tools.

In Focus This Week

1. Lead Article — AI Citations, Professional Duty, and Evidentiary Integrity

In May 2025, the Federal Court of Australia issued a costs penalty against Massar Briggs Law, which had acted for the applicant in a native-title determination proceeding. The Court found that a junior solicitor had incorporated generative-AI material into written submissions that contained fabricated case citations and non-existent authorities. When questioned, counsel admitted that no verification process had been applied before filing.

The judgment described the incident as a “serious lapse in professional supervision” and reminded the profession that the duty of candour to the Court cannot be delegated to software. The penalty, although modest in financial terms, was significant symbolically: it was the first recorded disciplinary consequence for unverified AI use within an Australian Commonwealth jurisdiction.

Across the Commonwealth, comparable warnings have emerged. In Canada, the Superior Court of Justice (Ontario) recently ordered lawyers to certify that no AI-generated content has been filed without verification.

The Law Society of England and Wales has issued guidance emphasising human oversight and audit trails. Singapore’s courts have taken a similar stance, reminding practitioners that AI tools are aids, not authorities.

The common thread is evidentiary: courts are drawing a bright line between assisted drafting and verified submission. Generative AI can propose language, but it cannot attest to authenticity, provenance, or privilege. Those remain human responsibilities.

For legal technologists and forensic practitioners, the case is a cautionary example of how digital efficiency must be balanced against professional duty. It also underlines why evidentiary integrity—particularly in emerging areas such as crypto tracing—demands transparent verification methods that can be explained in court.

Lexcrypta Perspective

At LexCrypta, we believe automation should never outrun accountability. Our verification framework ensures that every digital-asset report, attestation, or analytical statement is reviewed and digitally signed by a verified professional before release. Each deliverable carries a cryptographic proof-of-existence recorded on blockchain, allowing external parties to confirm that the document presented in evidence is identical to the version issued.

The purpose of this safeguard is not marketing —it is procedural integrity. When courts scrutinise the chain of custody for digital evidence, a verified identity and immutable timestamp are far more persuasive than an algorithmic assurance.

The full article can be found here, **Melbourne law firm caught using fake AI citations (IA ACS)**

2. Trend Watch — AI, Fake Citations & Professional Sanctions

Massar Briggs in Australia is not alone. Courts in multiple jurisdictions are now confronting the fallout from AI hallucinations in legal drafting.

Below are recent examples:

- ***Victoria, Australia*** — In a criminal matter, a senior counsel submitted AI-derived material containing fabricated quotes and later apologised to the Court. ABC News Report
- ***United Kingdom*** — The High Court warned lawyers they may face sanctions for filing AI-generated case references that do not exist. Reuters Coverage
- ***United Kingdom*** — In one case, of 45 citations submitted, 18 were later found to be fabricated. The Guardian Report
- ***United States*** — Mata v. Avianca (SDNY) — Two New York lawyers were fined US $5,000 after submitting a brief containing six fictitious cases generated by ChatGPT. The Court held that "reliance on an AI tool does not excuse failure to verify," marking the first formal sanction in the U.S. for AI-fabricated citations. Read more here.

These incidents suggest a pattern:
Courts are issuing real penalties for unverified AI use and the era of trusting AI as a research substitute is ending. What remains essential is verified authorship, human accountability, and audit-ready documentation.

3. Case Law Watch — UK Court Rules That Cold Wallets Are Recoverable Property

A UK High Court ruling confirms that cold wallets are legally "recoverable property." The decision strengthens the legal status of crypto under English law but warns that successful tracing still depends on evidentiary proof—not just blockchain visibility.

Key Findings
Crypto as Property
The High Court has confirmed that *Tether (USDT)*, a crypto-token, is considered "property" under English law, fitting into a third category of personal property — neither a *chose in possession* nor a *chose in action*.

It is not merely data; it represents a transactional right recognized by law, with the same proprietary expectancies as tangible assets.

Traceability Recognized in Principle
The Court reaffirmed that crypto assets can be traced or followed through blockchain transactions and are capable of being held on trust.

This confirms that established legal frameworks for tracing — fraud, misappropriation, and constructive trust — extend to digital tokens.

Tracing in Practice Requires Evidence
While the legal principle was accepted, the claimant in this case failed to demonstrate that the misappropriated USDT reached the defendant exchange's wallet.

The Court therefore dismissed recovery, underscoring that *traceability in law is not the same as proof in fact.* In short: without verifiable blockchain evidence, tracing fails.

Legal Context
This ruling builds upon the UK Law Commission's 2023 "Digital Assets" Report, which recommended formal recognition of digital assets as a distinct form of property.

It aligns with the proposed Property (Digital Assets etc.) Bill, currently before Parliament, designed to codify the proprietary status of digital assets and give statutory footing to existing case law.

Together, these developments confirm the UK's lead among Commonwealth jurisdictions in defining crypto-asset property rights — a model likely to influence Australia, Singapore, and Canada in upcoming reforms.

Implications for Lawyers
Practitioners can now treat most cryptocurrencies, including USDT, as traceable property capable of being held on trust or pursued under fraud.

However, successful tracing demands evidentiary rigor — transaction paths must be independently verified, with demonstrable links between wallets.

LexCrypta's mission is to provide the professional tracing tools and evidentiary documentation that meet this standard: human-verified reports, digital signatures, and blockchain proofs of existence suitable for inclusion in affidavits and pleadings. Read full article here.

4. From the Vault — Can You Subpoena MetaMask? Here's What We Know - Jurisdiction United States

MetaMask remains one of the world's most widely used non-custodial wallets.

By design, users—not MetaMask or its developer ConsenSys—control their private keys. That independence is core to its appeal but creates a difficult legal question: can you subpoena MetaMask for user data or transaction history?

The SEC took a swing and then walked it back. In June 2024, The U.S. Securities and Exchange Commission issued a subpoena to ConsenSys, alleging that MetaMask's *Swaps* and *staking* features effectively made it an unregistered securities broker.

Early 2025 — The SEC dropped the action, confirming MetaMask had not breached securities laws. The matter concluded without fines or findings of misconduct.

The case revealed a critical legal distinction: while MetaMask facilitates interaction with blockchains, it does not hold client funds or private keys, and therefore does not operate as a custodian.

Why does this matters for Legal and Compliance teams? Non - custodial architecture — MetaMask doesn't hold user assets; it merely provides an interface. Without "possession or control," it falls outside the legal definition of a custodian.

Limited transaction oversight — MetaMask cannot access comprehensive logs of user transactions or private wallets. Only individual users can export their data or sign proofs.

Traceable, but only via public data — Transactions visible on public blockchains can be traced; however, internal wallet metadata, user identities, and browser-side details remain beyond reach.

What This Means for Subpoenas
You can't subpoena MetaMask for unknown user keys or generic transaction records. It does not possess that data.

You can subpoena individuals — If a specific wallet address, email, or signing key is identified, the individual holder may be compelled to produce export logs or provide consent to disclosure.

Public blockchain data remains the best evidence — That's where forensic tools like LexCrypta Verify come in: converting publicly verifiable transaction flows into admissible, court-ready reports.

✅ **Legal Takeaway**
"MetaMask cannot be subpoenaed like a centralised exchange due to its self-custodial design. Legal tracing must focus on known wallet addresses and public blockchain evidence. The SEC's withdrawal confirms: custody requires control of user keys, not software intermediaries."

📌 **SEC Press Release — April 2024:**
The U.S. Securities and Exchange Commission clarified its position on ConsenSys and MetaMask's brokerage status. Read the official SEC release here.

About Lexcrypta

Lexcrypta Global assists law firms, trustees, and regulators in the forensic tracing and recovery of digital assets.

We specialise in:

- Blockchain forensics and asset recovery
- Subpoena and disclosure support
- Vault custody for court-managed assets
- Verification and audit attestation for crypto holdings

This is a Lexcrypta verified communication.
This publication is authenticated through Microsoft Entra ID and encrypted.

Proof for integrity verification.
Proof Key #0001-Oct25 | lexcrypta.com

Request a chambers briefing on AI verification and crypto tracing.

Next month:

What is the difference between a hot and cold wallet?

What happens if crypto is on an exchange and in pooled funds?

Is it worth recovering?