THE INSUMER MODEL LLC
New Canaan, Connecticut, USA
douglas@insumermodel.com | insumermodel.com

September 25, 2026

Innovation Task Force
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581

Via email: Innovation@cftc.gov

Re: Authorization and records when software acts for a customer

Dear Members of the Innovation Task Force:

The Insumer Model LLC submits this written input on a question within the Commission's focus on artificial intelligence and autonomous systems: when software acts for a customer, how can the parties show later that the software's authority was in force at the moment it acted, and what record will support that? The question will come up more often as customers direct automated systems, including AI agents, to act for them. We offer it ahead of the Task Force's October 28, 2026 forum on artificial intelligence and agentic finance.

The Insumer Model operates InsumerAPI, a service that checks whether a blockchain wallet address meets a condition set by the relying party and returns a digitally signed yes or no. One of the conditions it can check is whether a delegation that a principal has granted to another wallet on a public blockchain is validly signed by that principal, has not been revoked, and is within any time limits it carries. Each attestation it returns is signed with both ECDSA and ML-DSA, and a digest of the statement linking the two public keys is recorded on a public blockchain. We sell this service, and we ask that our comments be read with that interest in mind. We have made related points to the Securities and Exchange Commission in a comment on File No. 4-927 (September 17, 2026), available at https://www.sec.gov/comments/4-927/4927-1052439-3612229.pdf, in written input to its Crypto Task Force (September 25, 2026), available at https://www.sec.gov/files/ctf-written-memo-douglas-c-borthwick-insumer-model-092526.pdf, and in a comment on File No. S7-2026-27 (September 25, 2026).

1. An open question about authority and timing

Rule 166.2 (17 CFR 166.2) provides that no futures commission merchant or introducing broker may effect a transaction for a customer's account "unless before the transaction" the customer, or a person the customer has designated to control the account, has specifically authorized it or has given written authorization to trade without specific authorization. In the ordinary case, a customer's own orders are specifically authorized, and discretionary trading rests on a written authorization given in advance.

Software acting for a customer may not fit neatly into either case, and we do not suggest how the rule should apply to it; that is a question for the Commission and its staff. We note only a practical feature

of these arrangements that bears on it. A customer may give an automated system authority that is limited by amount, instrument, or time, and may narrow or withdraw that authority at any point. The customer's authority to the software is a separate matter from the customer's authorization of the futures commission merchant or introducing broker, and it may change more often. Where it is expressed as a signed delegation on a public blockchain, its status at a given moment can be checked against the chain: whether it was signed by the key that controls the customer's wallet, whether it has been revoked, and whether its time limits are met. If the Task Force considers how existing rules apply to orders originated by software, the time at which that authority is checked, and the record of the check, may be useful points to address.

2. The record of the check

Rule 1.31(c)(2) (17 CFR 1.31(c)(2)) requires a records entity keeping electronic regulatory records to establish systems and controls that ensure their authenticity and reliability, including "[s]ystems that maintain the security, signature, and data as necessary to ensure the authenticity of the information contained in electronic regulatory records." Where a party checks, before an action, that a customer's delegated authority is still in force, a record of that check should state the authority relied on, the account or wallet it covers, the time of the check, and the outcome, and should carry a digital signature that can be verified against a published public key. A record of that kind could form part of the systems the rule describes. It can be verified independently of the systems that produced it, provided the public key, and evidence of when that key was in use, remain available.

Staff's updated FAQs of September 24, 2026, available at https://www.cftc.gov/media/14671/FAQ_CryptoAsset092426/download, make a related point about records kept on a blockchain. CFTC staff would not object to records created and maintained on a blockchain, provided the records entity can fully satisfy the requirements of Rule 1.31. Where an entity uses a public and permissionless network for recordkeeping, "it should establish systems and controls that enable it to retain and produce such records under any circumstances, including in the event of an emergency or other disruption to the network (or its associated block explorer)." The same concern, that a record remain usable if a particular system is unavailable, applies to records of checks made against a blockchain.

3. How long the signature must last

Rule 1.31 requires most regulatory records to be kept for at least five years, and records of a swap until the swap terminates or matures and for at least five years after that. A five-year record made in 2031 must be kept until 2036, and records of long-dated swaps may need to be kept far longer. NIST's draft transition plan (NIST IR 8547, initial public draft, November 2024) lists ECDSA, a signature algorithm in wide use today, as "Disallowed after 2035" because it is expected to be vulnerable to quantum computers. Once a signature algorithm can be broken, a signature made with it can no longer, on its own, show that the record is authentic and unchanged, including the time it states. Signing with an algorithm standardized in FIPS 204 (ML-DSA), alone or alongside a classical signature, is one way to address this with standards available today.

4. Suggestions

As the Task Force develops its thinking on automated and agentic trading, we suggest it consider:

(a) whether parties relying on software acting for a customer should be able to show that the software's authority was in force when each action was taken;

(b) whether a digitally signed record of such a check, verifiable against a published public key, can form part of the systems that ensure authenticity under Rule 1.31(c)(2); and

(c) that, where records must be kept for many years, the signature or other method used to ensure authenticity should be expected to remain secure for the whole retention period.

Thank you for considering these views.

Respectfully submitted,

/s/ Douglas Borthwick
Douglas Borthwick
Founder, The Insumer Model LLC
douglas@insumermodel.com