AuthentiDate's Proposed USPS EPM-based solution to Mutual Fund Timing

One way to solve the problems outlined by the SEC is to establish a "time-stamp clearinghouse", which would be regulated by the SEC, and which would enforce the 4:00 PM trading cutoff. The challenge is to design a system that would allow the major funds traders to securely time-stamp trades at very high transactional rates as close to the 4:00 close as possible while still being able to prove to the SEC that time-stamps are neither tampered, added, or deleted after 4:00 PM to prevent late processing and market timing abuses.

The total number of mutual funds transactions is approximately 230M trades per day. If 80% of these trades are to be performed between 3:30 and 4:00 the peak transaction rate would be about 6M trades per minute, or 100K per second.

This rate would likely exceed the capabilities of any centralized solution that involved transmitting the entire order contents to the clearing house prior to the 4:00 PM close, forcing the firms to cut off trading earlier (as early as 10 AM) in order to get them time stamped prior to 4:00 PM. This would put the customers of these funds (especially 401K funds) at a distinct disadvantage in the market. However, ***a solution based on batched hash code checking and multiple secure high performance time stamping servers could handle this type of peak volume and allow trades right up to the 4:00 close.***

The approach suggested provides the clearinghouse with its own USPS EPM data center, with as many time stamp servers, application servers, and database servers as is necessary to handle the peak volume.

Batching for Improved Efficiency

Time stamping hundreds of millions of individual hash codes in the space of a few minutes would be a daunting challenge for today's hardware security modules and time stamping solutions, which typically can issue only several hundred timestamps per second per device. Handling 100K trades per second could require hundreds of devices if each trade were time stamped separately. Fortunately, The EPM Service supports "batching" of hash codes, whereby a particular order processing system at a fund trader could accumulate orders and periodically send them to the clearing house for time stamping. The entire batch would be issued a single time stamp, thus greatly reducing the number of time stamp servers required. NOTE: The USPS has a patent pending on this batching process, which it calls "Micro EPM".

The Problem

- Need a way to check that the intent order is not altered, deleted, or inserted after the 4:00 PM close. The SEC seems to strongly prefer that this checking be done by a trusted third party and not by the firms themselves.
- Need a way to check that execution of the intent orders is carried out appropriately. Execution is a complex, rule driven process. But if firms can create automated systems that do execution, a trusted third party should be able to duplicate the process, provided the rules

can be coded in a standard rules language, and the rules that will be used to determine the execution should be received prior to 4:00 PM (if there are any changes from prior day). Since execution can be fraudulently tampered with as easily as intent orders can be, a complete solution would require a trusted third party to be able to check execution integrity as well as intent order integrity.

Centralized Solution

A centralized solution would involve a central USPS EPM time stamping and non-repudiation service built at the clearinghouse, plus additional systems that perform the checking processes outlined below utilizing the EPM system for time-stamping and non-repudiation. It is important to note that the time-stamping requirement is to prove that trades are originated ("intent orders") prior to 4:00 but the exact time each transaction originated is not as important (unlike the stock market where exact timing is crucial). This key difference makes is possible to "batch" multiple orders and issue them a single shared time-stamp and still satisfy the SEC, as long as it is possible to prove that intent orders are not altered, created, or deleted after 4:00 PM, and additionally that the execution of these orders is consistent with the intent orders.

A possible scenario:

Intent Order Checking

1. Firm creates a batch of intent orders of any size (one to thousands or even millions of intent orders).
2. All intent orders are stored by firm and must not be subsequently altered. Execution of the intent order will be associated with the intent order but the intent order never changes.
3. Each order in the batch is hashed.
4. All hashes are combined in a single batch file.
5. Batch file of hashes is signed by the firm and sent via EPM protocol to clearinghouse for time stamping.
6. The clearinghouse stores the batch and issues a signed time-stamp for the batch (time-stamp actually signs a "super-hash" of the batch file).
7. Time-stamp and a unique transaction ID are returned to firm as proof of when they submitted the batch.
8. After 4:00 PM and before 6:30 AM the firms send all intent orders in the batch to the clearinghouse tagged with the transaction ID.
9. Clearinghouse runs a check program that hashes each intent order, then does a batch compare of these hashes against the hashes submitted prior to 4:00 PM.
10. An exception report flags any mismatches in the batch. This catches modified intent orders.
11. After all orders have been received, an additional program generates an exception report of any batches that were time-stamped prior to 4:00 PM for which no actual intent orders were received. This prevents firms from deleting trades and catches lost orders.

Execution Order Checking

This is a tougher problem, as the execution of orders is a complex, rule driven process that varies from firm to firm. If the clearinghouse receives all intent orders and also eventually receives the execution of that order, it might be possible for each firm to submit a list of edit rules they use to

determine executions (market prices of stocks and rules for deciding how to execute each type of trade) in a language such as ebXML or a language defined for the purpose in XML. The rules would be fairly static (and would have to be received prior to 4:00 PM to avoid "changing the rules" to defraud the system) and execution prices could be submitted to clearinghouse after execution prices are finalized each day. The clearinghouse could then take each intent order, apply the appropriate rules and execution prices, and recalculate the execution price. This would then be compared to the reported execution and an exception report would be created with mismatching executions.

Human order checking vs computerized checking

If it is not possible to check all execution orders programmatically by a trusted third party, orders could be pulled at random and checked by human auditors. If a large percentage can be automatically checked but the most complex types require human checking, a hybrid approach could check simple orders programmatically and have human audits of a percentage of the most complex orders.

100% checking versus random spot checking

The above approach still requires high volumes of data to be sent to the clearinghouse, even though they can be sent overnight. An elaboration of the scheme would have the clearinghouse randomly select batches from all received hash code batches for audit. In this scheme, the clearinghouse server would request the batches as needed versus the firm pushing all batches to the clearinghouse. The drawback of spot checking is it will not produce a guaranteed exception report of all mismatched or missing intent orders. However, if a high enough percentage of transactions are audited, it will act as a significant deterrent to fraud.

Distributed Solution

This is similar to the centralized approach except that the batches could be held at each firm and only a super-hash of the batch would be sent to the clearinghouse prior to 4:00 PM for time-stamping. After 4:00 the firm would send the batch of hashes and this would be compared to the previously sent super-hash. From this point the process would continue as in the centralized approach.

The big drawback of relying exclusively on the super-hash is that if there is a mismatch, ALL transactions in the batch are suspect (It will not be possible to prove that any of the hashes are valid in the batch if a single hash mismatches).

Process Flow Diagram – Intent Checking

The following diagram illustrates how the intent checking process would work: