US regulators propose powers to scrutinise algo traders' source code

Gregory Meyer in New York and Philip Stafford in London

©Bloomberg

Futures trading is dominated by computers, and nothing is more valuable than the "source code" of these high-powered machines.

Trading groups zealously safeguard this ever-evolving code — which they call their "secret sauce" — in online "repositories" that strictly control a coder's access.

IN Trading Technology

But US regulators want access to such information as they seek to reduce the risk of a trading accident. It is a proposal that alarms the industry and its ranks of automated trading firms.

Under a rule proposed last week, source code repositories would be open to inspection by the Commodity Futures Trading Commission and the US Department of Justice without a subpoena.

The idea of sharing source code with government officials is emerging as the most controversial element of the CFTC's new regulation on automated trading — Reg AT for short — which attempts to catch up with the explosion in automated trading over the past 10 years.

"While we think that the CFTC's goal is perfectly reasonable, it's inconceivable that any firm should be expected to leave its intellectual property on the doorstep of the government," says Bill Harts, chief executive of Modern Markets Initiative, a trading industry group, whose members include Hudson River Trading and Tower Research Capital.

While other elements of the 521-page document will elicit debate, source code raises hackles because of its inherent secrecy and the federal government's history of cyber security.

The concerns are twofold. One is that source code obtained by the government might inadvertently wind up in the hands of third parties. In 2011 Bernie Sanders, the Vermont senator, released confidential CFTC data identifying traders with large oil and gas positions, vexing some.

In 2012 exchange operator CME Group alleged that CFTC economists had published reports that revealed individual customers' positions. More recently hackers in China breached the US Office of Personnel Management and obtained records of more than 21m federal employees — including those at the CFTC.

The other concern is that a government employee who has inspected a trader's source code repositories could pass through Washington's revolving door and share that lucrative knowledge with a rival trading firm.

Rob Creamer, chairman of FIA Principal Traders Group, said last week the industry group would "pay particularly close attention to the issue of access to proprietary algorithms".

According to two futures executives, some trading firms use GitHub of San Francisco as a source code repository service. GitHub says it does not disclose the code stored in private repositories without a search warrant.

Manual v automated in CME futures trading by product

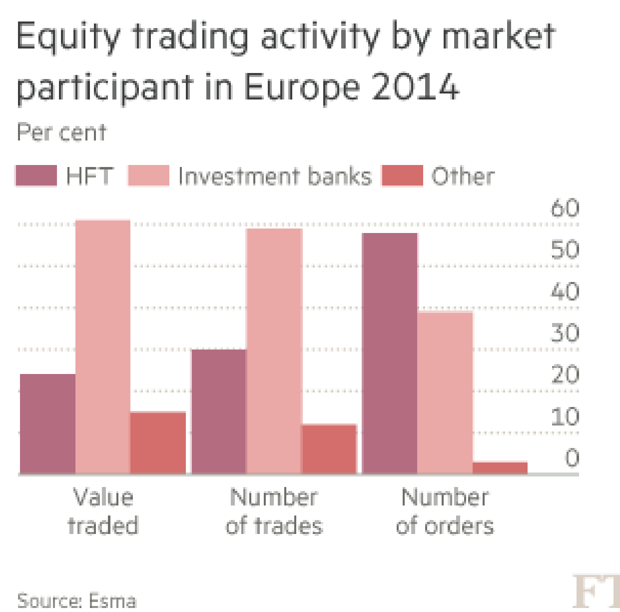
Product Group Name	ATS (%)	Manual (%)
Agriculture	38.1	55.6
Energy	46.9	36.4
Equities	66.6	32.5
FX	79.9	16.8
Interest rate	62.3	33.4
Metals	46.5	48.0

Source: CFTC (data compiled between November 2012 - October 2014)

The source code repository requirement is just one element of the rule proposal.

For the first time proprietary trading firms using algorithms to connect to exchanges directly would have to register with the CFTC, subjecting themselves to mandates such as throttles governing the number of orders a firm may place in a given time. Most firms already use such risk controls voluntarily, according to an FIA survey.

Others say the CFTC's rules bring the agency into line with standards and definitions on algorithmic trading that are coming into effect elsewhere in the industry, either in different asset classes such as US Treasury securities or in regions, including the forthcoming Mifid markets regulations in Europe.



"Save for some rules around wash trades, there isn't anything really we haven't seen in Europe already, although the devil will be in the detail," says Sam Tyfield, a lawyer at Vedder Price in London.

"The rules say EU-registered firms must keep records of any changes they make to any software used for trading for five years, which arguably amounts to them keeping the source code."

Even so, he acknowledges, it is likely to be a sensitive issue in the US.

As the CFTC's proposal was unveiled, global supervisors released their own consultation paper on cyber resilience for financial market infrastructures.

A report by the International Organisation for Securities Commissions and the Bank for International Settlements says critical market infrastructure such as exchanges and clearing houses should be encouraged to consider keeping data secure via encryption.

The CFTC proposal outlined the risks of an out-of-control automated trading system, citing the role of a faulty automated execution algorithm in the 2010 "flash crash", and glitches hitting Knight Capital on the equities market and Goldman Sachs in options trading.

Rick Lane, chief executive of Trading Technologies, a US software vendor, says: "More and more computers and fewer humans make trading decisions as time goes on."

But the rules will not solve the problem of sudden crashes and sharp rises, he adds. “I suspect that even if we get better at preventing them, the number will still remain relatively constant [because software] is not a perfect science.”