Pre & At-Trade Risk Management and Post-Trade Market Surveillance Systems

Modulus®

Solution Overview

T. +1(480) 525-7940
Scottsdale, AZ 85260 USA
www.modulusglobal.com

Modulus Market Surveillance & AML

The Modulus Market Surveillance, Risk Management & Anti-Money Laundering system utilizes Machine Learning to prevent and monitor the following abuse patterns:

Front Running

Spoofing & Layering

Quote Stuffing

Momentum Ignition

Hammering

Churning & Wash Trading

Money Laundering

Illicit Funds Detection

How It Works

Front Running Mitigation

Fund managers may require several days to execute large orders. Typically, someone within a trading firm or exchange may know that a large order is being executed and could potentially use that knowledge for their own personal gain through a process known as front-running.

Front running is when someone enters into a trade on the basis of (and ahead of) an order that is being carried out for a client.

Modulus employs Machine Learning to analyze markets for small changes that may correlate to front running of large trades. Whenever trading patterns that correlate to front running are identified on the exchange, the exchange operator receives an alert to investigate the matter.

How It Works

Spoofing & Layering Mitigation

Spoofing is a disruptive trading activity employed by traders to outpace other market participants and to manipulate markets. Spoofers feign interest in trading, thereby creating an illusion of exchange pessimism in the market when many offers are being cancelled or withdrawn, or false optimism or demand when many offers are being placed in bad faith. Spoofers bid or offer with intent to cancel before the orders are filled. The flurry of activity around the buy or sell orders is intended to attract other traders to induce a particular market reaction such as manipulating the market price of a security. Spoofing can be a factor in the rise and fall of the market and can be very profitable to the spoofer who can time buying and selling based on this manipulation. Under the 2010 Dodd-Frank Act in the US, spoofing is defined as "the illegal practice of bidding or offering with intent to cancel before execution." Spoofing can be used with layering algorithms and front-running, activities which are also illegal. High-frequency trading, the primary form of algorithmic trading used in financial markets is very profitable as it deals in high volumes of transactions. Modulus identifies spoofing & layering by observing the patterns of traders. When traders cancel more than a certain percentage of orders (which can be defined), the system creates an alert for the exchange operator to investigate the behavior immediately. Traders may be warned or banned.

How It Works

Quote Stuffing Mitigation

Quote stuffing refers to a form of market manipulation employed by API traders that involves quickly entering and withdrawing a large number of orders in an attempt to flood the market. This can create confusion in the market and it can create trading opportunities for high-speed traders. By quote stuffing, trading systems delay price quotes while the stuffing is occurring, simply by placing and canceling orders at a rate that substantially surpasses the bandwidth of market data feed lines or the matching engine. The orders pile up in buffers and the delay (increased latency) lasts until the buffer drains. It has been established that quote stuffing occurs frequently – when thousands of replacement orders for one market are crammed into a second, each order is valid for less time than it takes for the news of the order (traveling at close to the speed of light) to reach anyone not at the exchange; no one can execute a trade against the phantom order. Modulus identifies quote stuffing by observing the patterns of traders. When traders cancel more than a certain percentage of orders via the trading API, the system creates can reject the orders in the Pre and At-Trade Risk Management process or can also create alerts for the exchange operator to investigate the behavior. Traders may be warned or suspended automatically by the system.

How It Works

Momentum Ignition Mitigation

Momentum ignition refers to a market manipulation strategy that attempts to trigger a large number of trades from multiple market participants in order to cause rapid price movements. This abuse method is similar in concept to spoofing and layering, except that instead of merely creating orders and canceling them, actual trades are processed. This method is also known as “pump and dump.” By instigating multiple traders to buy or sell quickly, the manipulator can profit either by having taken a pre-position or by laddering the book, knowing the price is likely to revert after the initial rapid price movement. Momentum Ignition is extremely difficult to detect and requires the use of machine learning. Modulus uses machine learning to identify potential patterns of momentum ignition between groups of traders within the Post-Trade Surveillance process. When repeat traders are found to be connected with similar trading behavior, the system tags the traders as potentially belonging to a Momentum Ignition Group and creates an alert for the exchange operator to investigate the behavior and take disciplinary action on a case by case basis.

How It Works

Hammering Mitigation

Hammering is rapid and concentrated selling by traders who perceive a market to be overvalued. Sometimes this is a natural trading phenomenon, but it can also be a sophisticated orchestrated abuse pattern. Similar to Momentum Ignition, Hammering can be extremely difficult to detect and requires the use of machine learning. Modulus uses machine learning to identify potential patterns of hammering between groups of traders within the Post-Trade Surveillance process. When repeat traders are found to be connected with similar trading behavior, the system tags the traders as potentially belonging to a Hammering Group and creates an alert for the exchange operator to investigate the behavior and take disciplinary action on a case by case basis.

How It Works

Churning & Wash Trading

Churning and wash trading are forms of market manipulation in which a trader simultaneously sells and buys the same financial instruments to create misleading, artificial activity in the marketplace. First, a trader will place a sell or buy order, then place an opposite buy or sell order to take the trade from himself. This may be done for a number of reasons:

> To artificially increase trading volume, giving the impression that the instrument is more in demand than it actually is.
>
> To generate commission fees to brokers in order to compensate them for something that cannot be openly paid for. This was done by some of the participants in the Libor scandal.

Exchanges in most jurisdictions are mandated to detect this abuse pattern. Wash trading has been illegal in the United States since the passage of the Commodity Exchange Act (CEA), of 1936. Modulus identifies Churning & Wash Trading and permits exchange operators to curb wash trading via Pre and At-Trade Risk Management controls.

How It Works

Money Laundering Mitigation

Digital Money Laundering is the process of concealing the origins of digital assets obtained illegally by passing it through a complex sequence of tumblers and exchanges. The overall scheme of this process returns the money to the launderer in an obscure and indirect way. Money laundering occurs on digital assets exchanges when traders intentionally lose money on trades while intentionally permitting specific other traders to recover the lost trades.

The Modulus Anti Money Laundering (AML) system identifies the top percentage of traders who consistently lose money while specific other traders gain the money and flags both as suspicious for money laundering. This is what we call "intentional pass-through trade losses."

The system also identifies the average total per-user deposit size and the average total number of traders per user, over a sliding window of time. If any user has deposited more than the n-th percentile of the average deposits, or has requested to withdrawal more than the n-th percentile of average withdrawals, then the user is again flagged as suspicious for money laundering, only if the user has not placed at least the average number of trades that would be expected for a trader who has deposited roughly the same amount of funds into the exchange.

How It Works

CipherTrace Integration

Modulus has partnered with the CipherTrace platform to provide a broad, high-resolution view of the cryptocurrency transaction landscape. We use this view to provide actionable intelligence for AML investigation and compliance within cryptocurrency exchanges.

CipherTrace integrates both open and closed-source intelligence, and leverages machine learning algorithms to rapidly aggregate and correlate a variety of indicators, and then provides users with actionable attribution.

Integration with Chainanalysis is also available.

Clients

For over 20 years, Modulus has provided advanced technology products and services to corporate, educational, governmental, and non-profit institutions clients in over 90 countries.

Modulus financial technologies are used by over three million traders / investors in 94 countries including brokers, hedge funds, financial institutions, and professional traders

Additionally, Modulus has used its HPC and ML expertise to developed solutions for clients in a wide variety of other industries

Top Customers Include:

- Goldman Sachs
- JP Morgan Chase
- Merrill Lynch
- NASDAQ

Merrill Lynch
Goldman Sachs
Smith Barney citigroup
GEDİK Investment
mantara
Credit Suisse
CBOT
Shell Exploration
SCTM
Chicago
MIT
R.J.O'Brien Established in 1914
Barclays Capital
indigo
ScanTheMarket.com
Microsoft
NASA
Alfa-Bank
Chase
Bank of America
LYCOS
Yahoo! Finance
NASDAQ
Siemens
FXCM
MUFG
Ameritrade
Scottrade More broker for your money.
HSBC
Investopedia
QwillTrade
HOTSTIX
Dell
ODL Securities
MB Trading
GAIN
Genesis Securities, LLC.
CME Group A CME/Chicago Board of Trade/NYMEX Company
Deloitte.
the University of Greenwich
Emirates
FXSolutions Advantage, Trader.
Interbank fx
Currenex
investools
VHAYU
Zignals
Universidad Santa Maria
東京
Deutsche Bank
Rutgers
Standard
ING

Location

14850 N. Scottsdale Rd, Scottsdale, AZ 85254