Market Abuse Case Studies

NatWest Markets Spoofing in U.S. Treasuries

Market Abuse Case Study No:	**Name:**
004	NatWest Markets Plc
Offence:	**Detection Control:**
Spoofing U.S. Treasury bonds with U.S. Treasury futures	MAST Cross-Product Layering/ Spoofing Metric

TradingHub

NatWest Markets Spoofing in U.S. Treasuries

Market Abuse Case Study No:
004

Name:
NatWest Markets Plc

Civilian Authority:
U.S. Department of Justice

Offence:
Spoofing U.S. Treasury bonds with U.S. Treasury futures

Detection Control:
MAST Cross-Product Layering/ Spoofing metric

Findings:
NatWest's "materially false and misleading information was intended to... trick other market participants [into] buying and selling U.S. Treasuries at quantities, prices, and times that they otherwise likely would not have traded".

Key Facts

In 2021, NatWest Markets Plc pleaded guilty to wire and securities fraud following the discovery of unlawful spoofing schemes involving U.S. Treasury securities and Treasury futures by the U.S Department of Justice.

Between January 2008 and May 2014, a trader working in London for NatWest Markets Plc and a trader working in Stamford, Connecticut for the U.S.-based subsidiary NatWest Markets Securities Inc., independently "engaged in schemes to defraud" by manipulating U.S. Treasury futures contracts on the Chicago Board of Trade (CBOT).

A few years later in 2018, two traders employed by NatWest Markets Plc's Singapore branch also "engaged in schemes to defraud in connection with the purchase and sale of U.S. Treasury securities in the cash market."

On hundreds of occasions between 2008 and 2018, the traders placed one or more spoof orders on one side of the market whilst simultaneously placing one or more genuine orders on the opposite side. The spoof orders created an imbalance in the order book between the resting buy and sell quantities which exerted either upwards or downwards pressure on the price.

In most instances, the traders placed their spoof and genuine orders in the same instrument, whether U.S. Treasury or future. However, at least one trader took advantage of the shared underlying risk exposure between the two to use spoof orders in Ultrabond futures contracts to benefit their genuine orders in 30Y Treasury bonds.

Court Findings

The District Court of Connecticut ruled that the NatWest traders "knowingly, willfully, and with the intent to defraud placed orders to buy and sell certain U.S. Treasuries with the intent to cancel those orders before execution ('Spoof Orders')".

The deliberate placement and cancellation of so-called 'Spoof Orders' amounted to deception by misleading other market participants through "false and fraudulent pretenses and representations concerning the existence of genuine supply and demand for U.S. Treasuries."

Through these Spoof Orders, the traders "intended to inject materially false and misleading information about the genuine supply and demand for U.S. Treasuries into the markets, and to deceive other participants in those markets into believing something untrue, namely that the visible order book accurately reflected market-based forces of supply and demand."

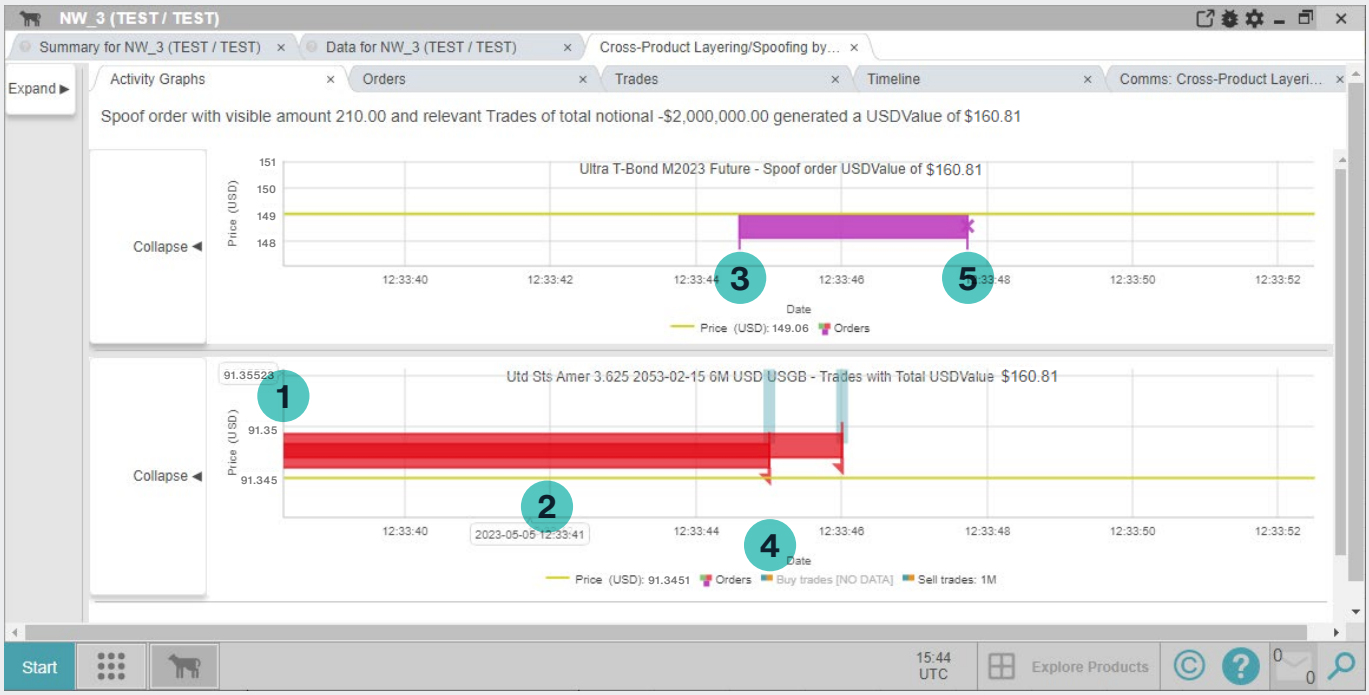
This "materially false and misleading information was intended to... trick other market participants [into] buying and selling U.S. Treasuries at quantities, prices, and times that they otherwise likely would not have traded". Ultimately, the trader's genuine orders benefitted from more favourable prices before the trader cancelled their spoof order prior to execution.

As a result, the court charged NatWest Markets with one count of wire fraud and one count of securities fraud. Under the resulting plea agreement, NatWest Markets agreed to pay $35 million comprising restitution, forfeiture and a criminal fine. Additionally, the bank agreed to serve three years' probation and take on an independent compliance monitor.

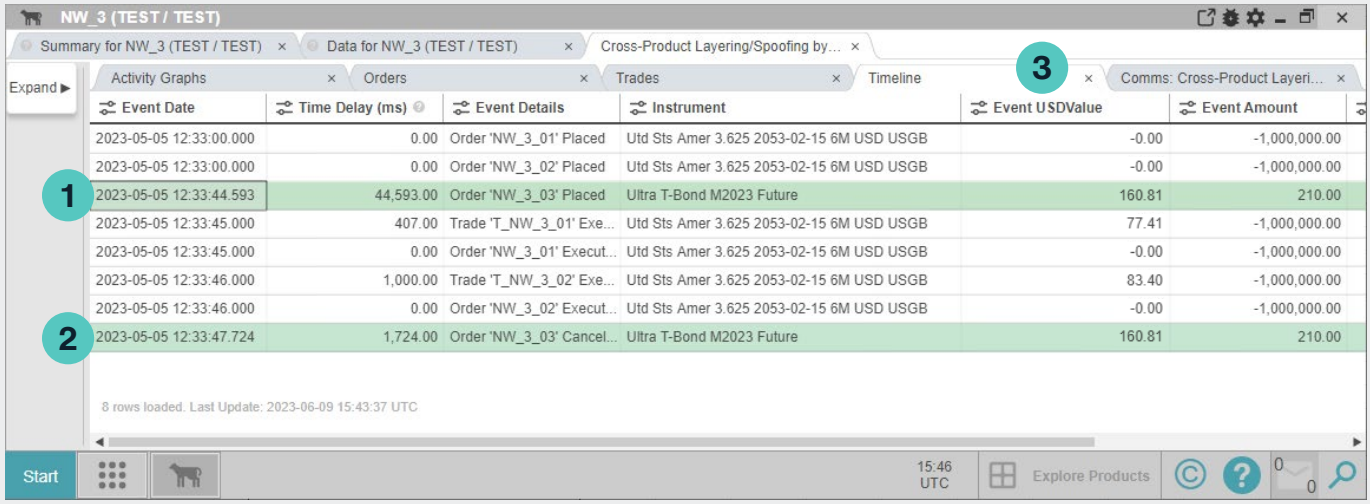
https://www.justice.gov/opa/press-release/file/1457981/download

Detecting spoofing with MAST

On May 14th 2014, a NatWest trader placed a spoof order to buy 210 Ultrabond futures contract in order to sell a total of 2,000,000 30Y U.S. Treasury bonds.



1. Around 12:33 pm, the trader entered several orders worth $2 million to sell 30-year U.S. Treasury bonds.
2. The orders went unfilled for several seconds.
3. At 12:33:44.593, the trader entered a spoof order to buy 210 Ultrabond futures contracts.
4. Almost immediately, they were able to fill their orders to sell U.S. Treasury bonds.
5. The trader cancelled their spoof order 3.131 seconds after having placed it.



1. The trader entered their spoof order at 12:33:44.593. Over the next 3.13 seconds, their genuine sell orders were all filled.
2. Once their sell orders had cleared, the trader cancelled their spoof order.
3. MAST calculates a severity score for each trade and order. In this instance, it has assigned the large spoof order a score of **$160.81**.

**The above is taken from MAST's Cross-Product Layering/Spoofing metric and constitutes a recreation of the original case.*

How MAST recognises spoofing

MAST's Layering/Spoofing metric detects spoofing by measuring the degree to which the market impact of a potential spoof order benefits any transactions on the other side of the market. It balances this benefit by also considering the risk to the trader of placing a spoof order, namely the cost to them of having to unwind an unwanted execution.

By measuring market impact, MAST is able to recognise that the trader's spoof order for 210 Ultrabond futures contracts exerted upwards pressure on the instrument's price from which his resting sell order in 30Y Treasury bonds benefitted. It derives its USD Value score for the instance by considering both the benefit to the sell order and the hypothetical cost of having to unwind his large spoof order. This lets it prioritise the most serious instances of spoofing for investigation.

How MAST detects cross-product abuse

MAST's general market modelling allows the system to understand how positions across a combination of instruments (bonds, futures, swaps etc...) and across a series of maturities are all linked and can share sensitivities to common factors – like the shape of convenience curve and the price of the spot for commodities, or the shape of the interest rate curve for rates.

At least one of the traders placed spoof orders in Ultrabond futures contracts to benefit sell orders in U.S. Treasury bonds. To detect such abuse, MAST recognises that the value of each Treasury is sensitive to changes in the dollar yield curve. It therefore links the trades and orders together through the hypothetical market impact they have on this yield curve.

THE CHALLENGES OF FIXED INCOME MARKET SURVEILLANCE SERIES

In **Part One**, we explore why fixed income is different, particularly in relation to cross-product abuse.

In **Part Two**, we explore market manipulation and how we might use market impact models to address the challenges of fixed income market surveillance.

In **Part Three**, we discuss market abuse utilising multiple products, also known as cross-product abuse, with a focus on the fixed income asset class.

Advance your surveillance function

Detect cross-product abuse, reduce false positives, and prioritise high-risk alerts.

Reach out to learn more.


tradinghub.com/MAST


tradesurveillance@tradinghub.com