Working Papers in Economics & Finance
2022-04

Cross-Market Spoofing

Alexis Stenfors, University of Portsmouth
Mehrdaad Doraghi, Features Analytics
Cristina Soviany, Features Analytics
Masayuki Susai, Shiga University
Kaveh Vakili, Features Analytics

Portsmouth Business School
https://www.port.ac.uk/about-us/structure-and-governance/organisational-structure/our-academic-structure/faculty-of-business-and-law/portsmouth-business-school

Cross-Market Spoofing

Alexis Stenfors[1], Mehrdaad Doraghi[2], Cristina Soviany[2], Masayuki Susai[3], and Kaveh Vakili[2]

[1] *Faculty of Business and Law, University of Portsmouth, Portland Street, Portsmouth PO1 3DE, UK. alexis.stenfors@port.ac.uk (Corresponding author)*

[2] *Features Analytics, Rue de Charleroi 2, 1400 Nivelles, Belgium.*

[3] *Shiga University, 1-1-1 Baba, Hikone, Shiga, Japan.*

Abstract

Since 2013, regulatory investigations have revealed widespread manipulation and collusive practices among banks active in over-the-counter (OTC) markets. These discoveries have resulted in fines and settlements amounting to billions of US dollars, criminal proceedings and stricter regulation worldwide. However, recent legal cases and regulatory reports indicate that authorities have stepped up their efforts to crack down on so-called "cross-market spoofing". The manipulative tactic involves a combination of a genuine order in one market and a spoof order in another, which is notoriously difficult to detect. In this paper, we use a high-frequency data set of limit order book snapshots from the foreign exchange (FX) spot market to develop and test a methodology to assess the feasibility, and hence potential prevalence, of cross-market spoofing. Our findings show that predictable reactions follow potential single-market spoofs that a market manipulator may exploit. However, we also find that predictability may be observed in closely related markets. In particular, we discover that EUR/JPY offers a reliable pathway for a manipulator to exploit via spoof orders at deeper levels in the EUR/USD or USD/JPY limit order books. Overall, our pilot study lends support to the increasing attention to cross-market manipulation by compliance officers and financial regulators.

Keywords: foreign exchange; limit order book; manipulation; market microstructure; spoofing; trading

JEL Codes: D4, F31, G1

1 Introduction

Since 2013, regulatory investigations into money market benchmarks, such as the London Interbank Offered Rate (LIBOR) and foreign exchange (FX), have revealed a widespread culture of manipulation and collusive practices among banks active in over-the-counter (OTC) markets. These discoveries have resulted in fines and settlements amounting to billions of US dollars, criminal proceedings and stricter regulation worldwide. More robust compliance mechanisms have also been implemented to identify and, hopefully, prevent such behaviour in the future (Stenfors, 2020; Stenfors and Susai, 2021). The development has prompted an urgent need for sophisticated surveillance technology by financial institutions, exchanges, trading platform providers and regulators. Indeed, surveillance technology has become the most frequently cited budget allocation among compliance departments (Nasdaq, 2019).

Trade surveillance is considerably more challenging for OTC markets, such as FX and fixed income, than exchange-traded equity markets. The decentralised and opaque nature of OTC markets makes it very difficult to source reliable data, which is crucial for the process. Moreover, compared to equity markets, OTC markets also tend to be extremely connected (Ilmanen, 1995; Sutton, 2000; Jotikasthira et al., 2015; Chatziantoniou et al., 2020, 2021). Traders are typically presented with a wide range of alternatives in terms of instruments, markets and venues when speculating on price changes in OTC markets or when hedging a portfolio. As such, trading is often less about the buying and selling of identical assets than about trading across related assets, instruments and markets. The abundance of different alternatives presents opportunities for traders to continually identify the instrument that offers the best value or best possible hedge. In addition, cross-market trading and hedging enable them to buy time, as the price of an instrument temporarily out of line is expected to converge towards its benchmark later.

The flip side is that it may also open the door for cross-market manipulation in general, and cross-market spoofing in particular. Two key arguments explain the logic of spoofing one market with the intent to profit from the reaction in another market. First, due to relatedness among markets but differences in liquidity, cross-market spoofing might involve less market risk and hence be cheaper than single-market manipulation (the hedging argument). Second, because the number of potentially related assets is vast, the perpetrator is considerably less likely to get caught (the detection argument).

However, as far as we know, no academic studies have yet attempted to empirically

explore cross-market spoofing. In this paper, we do so by developing and testing a methodology to assess the feasibility of cross-market spoofing and its potential prevalence in global financial markets. We use an ultra-high-frequency data set of limit order book snapshots from the EUR/USD, USD/JPY and EUR/JPY FX spot markets. Different currency pairs are not identical yet are, by definition, closely related to each other. This makes the FX market an ideal laboratory for cross-market manipulation research.

The results confirm the hypothesis that the choice of spoof order size and aggressiveness – in relation to the market as a whole – is crucial for the ultimate outcome of the manipulative tactic. However, we also find that a predictable reaction can be observed in closely related markets. In particular, we discover that EUR/JPY offers a reliable pathway for a manipulator to exploit via spoof orders at deeper levels in the EUR/USD or USD/JPY limit order books. The broader implications of our pilot study are that it supports the notion that cross-market spoofing tactics may be considerably more widely adopted than previously thought. This is in line with recent legal cases and regulatory reports from fixed income and commodity markets, which strongly indicate that authorities have stepped up their efforts to crack down on various forms of cross-market manipulation (AMF, 2019; CFTC, 2020; DOJ, 2021; FCA, 2018). Academically, the paper is most closely related to work on financial market misconduct in general (e.g. Cumming et al., 2011; Cumming et al., 2015; Stenfors, 2020) and spoofing in particular (Lee et al., 2013; Stenfors and Susai, 2021). However, it can also be read in the context of empirical FX market microstructure focussing on order flow (Daniélsson et al., 2012; King and Rime, 2010; Lo and Sapp, 2010).

The remainder of the paper is structured as follows. Section 2 describes single and cross-market spoofing through the lens of the relevant academic literature and recent legal and regulatory cases. Section 3 provides an overview of the data and the methodological approach. The model and results are presented in Section 4. Section 5 concludes.

2 Background and Related Literature

2.1 Single-Market Spoofing

Pirrong (2017) defines price manipulation as 'intentional conduct that causes market prices to diverge from their competitive level'. Historically, the vast majority of regulatory and legal cases have involved trade-driven rather than quote-driven manipulation (Fox et

al., 2021). An simple example is "ramping", which involves heavy buying or selling of an asset with the intent to move the market and then to offload the position at a profit. The same goes for the academic literature, which generally covers manipulation involving schemes where actual buying or selling is central to the misconduct. However, financial markets have evolved dramatically during the last few decades – and some important changes include the rise of electronic limit order books, algorithmic and high-frequency trading (HFT). As a result, most activity in today's markets takes place via limit orders and quotes rather market orders and transactions. It is only logical that this has become reflected in how misconduct occurs in financial markets.

Spoofing is a form of quote-driven manipulation and involves creating a false impression of the supply and demand in the market. It is, therefore, a form of market manipulation (Cumming et al., 2011; Cumming et al., 2015). A spoofer intends to trick other market participants into believing that the market is bid, whereas the genuine interest is to sell – or vice versa. Consider the following hypothetical example of a spoofing strategy. Suppose the market for Asset A consists of buy orders amounting to 10 million (M) USD at 100.00 and sell orders of 10M USD at 100.05. Let us assume that a trader (the spoofer) enters the market and wishes to sell at the highest possible price. An example of a spoofing strategy would be the following. First, the spoofer submits a sell order of 2M USD at 100.04. This order is usually referred to as a "resting order" or "genuine order" because it is intended to be executed. Next, the spoofer submits a buy order of 30M USD at 99.98. This order is referred to as a "spoof order" because it is not intended to be executed. Although the best bid/ask price remains unchanged at 100.00-100.04 following the new order submission, the depth structure of the limit order book has changed dramatically. Subsequently, other traders notice the sudden increase in demand from the bid side and anticipate that the price of Asset A will increase. A successful spoof would entail that the genuine sell order of 2M USD is lifted at 100.04. Immediately after that, the spoofer exits the strategy by cancelling the 30M USD spoof orders at 99.98.

The example demonstrates that spoofing is a low-cost and low-risk strategy compared to other manipulation tactics. In contrast to ramping, for instance, it does not generate an undesirable position for the manipulator, which might prove difficult or expensive to offload in due course. Spoof orders, regardless of size, are never intended to be executed and are simply meant to lead other traders astray and react as if genuine orders have entered the market. Nonetheless, size and price aggressiveness are two critical ingredients

of any spoofing strategy. A limit order submission involves a strategic trade-off between the size and the aggressiveness of the order (Lo and Sapp, 2010). A large and/or aggressive order is more likely to trigger traders on the same side of the order book to improve their orders (due to "non-execution risk"). At the same time, traders on the opposite side of the order book are more likely to cancel their orders and resubmit them at less competitive price levels (so-called "free-option risk") (Fong and Liu, 2010; Liu, 2009). However, whereas a trader submitting a genuine limit order would prefer to minimise the impact stemming from the size and the aggressiveness to achieve the best possible execution, the objective behind a spoof order is to maximise the impact – whilst maintaining a minimal risk of execution. This implies that spoof orders ought to be large but relatively non-aggressive. Empirically, this is also confirmed by Lee et al. (2013), who conduct spoofing tests on exchange-traded stock market data. Stenfors and Susai (2021), however, find that spoof orders in liquid FX markets could be relatively small and aggressive – suggesting that optimal spoofing strategies might differ across markets and trading venues.

The 2010 Dodd-Franck Act explicitly made spoofing in the commodities and futures markets illegal in the U.S. Spoofing, here, is described as "bidding or offering with the intent to cancel the bid or offer before execution" (Mark, 2019). The arguments used to justify why spoofing is harmful are relatively similar to those concerning market manipulation in general – namely that it is detrimental to market integrity, market quality, market liquidity, market stability and the price discovery process (Fox et al., 2021; Mark, 2019; Stenfors and Susai, 2021). Although not explicitly outlawed in all financial markets and jurisdictions, recent years have seen a dramatic increase in regulatory investigations, fines and criminal proceedings related to spoofing around the world.

The most publicised spoofing case is undoubtedly that of Navinder Singh Sarao, colloquially often referred to as the "flash crash trader". Despite not being found to have caused the stock market flash crash of May 2010, the high-frequency trader's spoofing activities were deemed to have contributed to the turmoil. Indeed, the first spoofing investigations and regulatory settlements focussed almost entirely on markets with a high proportion of HFT and algorithmic traders (CFTC, 2018). Spoofing is a form of bluffing that existed long before the advent of computers. However, spoofing tactics require a comprehensive and often frequently repeated assessment of the prevailing market depth and liquidity, as well as the ability of submit and cancel orders fast. It is therefore not surprising that sophisticated technology has been central to the spoofing schemes, and

that exchanges or electronic limit order books have been the chosen venues – such as Citigroup and Mitsubishi UFJ Morgan Stanley Securities Co. in the Japanese government bonds (JGB) futures market (Securities and Exchange Surveillance Commission, 2018; Financial Services Agency, 2019). Further, in September 2020, JP Morgan was fined a record 920M USD by regulators for spoofing and manipulation of precious metals and U.S. Treasury futures contracts. According to a press release by the CFTC (2020), the activity by JP Morgan had "involved hundreds of thousands of spoof orders". Cases such as these demonstrate how relatively traditional markets are far from immune from quote-driven manipulation such as spoofing.

More recently, in December 2021, NatWest pleaded guilty to fraud in the U.S. Treasury markets (DOJ, 2021). The following example illustrates some of the activity related to the NatWest spoofing case: On 25 July 2012 at 10:05:01.416 a.m., a NatWest trader submitted a genuine order to buy 10 Ultra U.S. Treasury Bond Futures contracts at USD 175.90625. (The derivatives contract is linked to Treasury bonds with a remaining term to maturity of not less than 25 years.) 158.716 seconds later, the trader placed a spoof order to sell 500 Ultra U.S. Treasury Bond Futures contracts at USD 175.93750. The intent of the spoof order was to create an illusion of supply, in other words, to deceive other market participants into believing the price was likely to fall. After 24 milliseconds, the trader's genuine order was filled. 858 milliseconds later, the trader cancelled their spoof order.

2.2 Cross-Market Spoofing

Traditionally, it has been assumed that spoofing takes place in a specific asset (a stock or bond, say), resulting in a price change in the same asset. Problematically, a spoofing strategy could also involve a combination of a genuine order in one asset and a spoof order in another asset. There are two main reasons why a spoofer might adopt what might seem like a much more complex strategy. First, because of the vast number of cross-asset or cross-market combinations, detecting such a spoofing case is more challenging. Thus, from the spoofer's perspective, the risk of detection is considerably smaller. Second, cross-market manipulation might expose the spoofer to less market risk and hence be cheaper than single-market manipulation due to relatedness among markets but differences in depth and liquidity. The logic is similar to hedging. To minimise transaction costs, traders typically seek the cheapest possible hedge among assets or instruments that are

considered to be most liquid – yet closely related to the asset to be hedged. For instance, a futures contract might be more widely traded and liquid than the underlying asset. If so, the futures contract could be seen as the most appropriate hedge and, from time to time, serve to replace trading that would take place in the underlying asset. Nonetheless, traders would follow both markets simultaneously and expect the futures contract as well as the underlying asset to move more or less in tandem.

A spoofer may turn this principle to his advantage. Consider, again, the example of Asset A earlier. The market is 100.00-100.05 with 10M USD on each side of the order book. A spoofer then enters the market and submits a genuine sell order of 2M USD at 100.04. Now suppose that there is an Asset B, which is closely related to Asset A. Market participants are aware that they tend to move together, implying that they closely follow the developments in both markets. For simplicity, let us assume that the market for Asset B is 90.00-90.05 with 10M USD on each side of the order book. An example of a cross-market spoof would involve submitting a buy order of 30M USD at 89.98 for Asset B (the spoof order). Again, the best bid/ask prices for Asset A and Asset B remain unchanged at 100.00-100.04 and 90.00-90.05. However, other traders notice the substantial increase in demand from the bid side of Asset B, which is closely related to Asset A. As a result, they anticipate not only that the price of Asset B will increase, but also the price of Asset A. A successful spoof would imply that the genuine order in Asset A gets executed, whereas the spoof order in Asset B is cancelled immediately thereafter.

The NatWest guilty plea in December 2021 included cross-market spoofing, as illustrated by the following scenario. On 14 May 2014 at 12:33:44.593 p.m., a NatWest trader submitted a spoof order to buy 210 Ultra U.S. Treasury Bond Futures contracts at USD 149.59375. The number of contracts is equivalent to 21M U.S. Treasury bonds with a maturity of 25 years or longer. The relatively large order submission intended to deceive others into believing that the futures price would go higher and, consequently, that the prices of underlying cash bonds would follow. 3.131 seconds later, the trader cancelled the spoof orders. In the meantime, the trader managed to get genuine sell orders of 2M 30-year U.S. Treasury bonds filled (DOJ, 2021).

The real-life example shows how the spoofing logic can be extended to involve manipulation in a cash instrument to profit from the impact on a futures contract or vice versa. In this instance, the futures market is deeper and more liquid than the cash market – allowing the trader to submit a larger spoof order than what would have been possible

in the cash market. At the same time, the relatedness between the two markets is exceptionally high. This means that market participants are likely to react to sudden changes in supply and demand in a similar fashion, regardless of whether the new signal comes from the cash or the futures market.

Such possible related pairs of two assets or markets are often reasonably easy to identify (e.g. U.S. Treasury bond vs U.S. Treasury Bond Future or Apple stock vs Apple Future). In April 2022, CFTC charged a trader and two firms with engaging in, inter alia, cross-market spoofing schemes. In this case, spoof orders had been placed in the soybean futures markets, whereas genuine orders were posted and executed in the related but less liquid options on soybeans futures market (CFTC, 2022). Indeed, the LIBOR and FX manipulation scandals overwhelmingly involved scenarios of such "vertical" manipulation within the same branch of a particular financial market. For instance, on numerous occasions, the JPY LIBOR benchmark was manipulated to profit from the impact it would have on JPY LIBOR-related financial instruments such as JPY forward rate agreements (FRAs) or JPY interest rate swaps (IRSs) (FCA, 2012). Fortunately, it is straightforward to map the relatedness between cash and futures contracts or between the 3-months JPY LIBOR and, say, a 1X4 JPY FRAs, which is fixed and settled against the 3-month JPY LIBOR.

Problematically, and in OTC markets in particular, the list of possible asset combinations is almost endless when not only vertical but also "horizontal" cross-market manipulation scenarios are considered. For instance, a frequently cited case study among financial regulators and market surveillance professionals is the so-called "Stevenson case", a Final Notice imposed by the FCA in 2014 (FCA, 2014). The case concerned a trader (Mark Stevenson) at Credit Suisse ramping the price of one particular Gilt (UK government bond) in relation to a range of other Gilts with similar, but not identical, maturities. A more recent high-profile case involved the French regulator AMF fining Morgan Stanley for manipulating French government bonds futures contracts (OAT Futures or FOAT) against various maturities of French and Belgian government bonds (AMF, 2019). The Morgan Stanley case is particularly important because it demonstrates that financial regulators have started to take notice of such horizontal cross-market manipulation. A similar message was conveyed by the FCA (2018), stating that "[. . .] some analysts tended to take a narrow approach, reviewing only the activity in the product which triggered the alert and not considering other trading in correlated products. Because many fixed income

products are inter-connected, consideration of trading activity in correlated products - such as cash vs futures, or products with different durations - is an important element of effective surveillance."

Thus, compared to equity markets, OTC markets involving bonds, interest rate derivatives, and FX tend to be extremely connected (Ilmanen, 1995; Sutton, 2000; Jotikasthira et al., 2015; Chatziantoniou et al., 2020, 2021). This makes them particularly susceptible to cross-market manipulation and spoofing. A 10-year German government bond may, for instance, be related to bonds with similar maturities issued by the German government or even other issuers of equal credit standing. The relatedness also stretches to futures, options, swaps and so on. The same goes for the FX market, where one currency is traded against another – creating a "universe" of currency pairs related to each other.

3 Data and Generation of Spoof Events

3.1 Data

In this pilot study, we develop and test a methodology to assess the feasibility of cross-market spoofing – and hence the potential prevalence of such misconduct in global financial markets. We use 'EBS Level 5.0' data and analyse three FX spot currency pairs from 1 October 2013 to 28 February 2015. EBS is the most commonly used platform by market-making banks and high-frequency traders and is particularly strong in the major currency pairs. All activity on EBS is done by institutional traders (retail and non-institutional traders do not have access to the platform). We have chosen EUR/USD, USD/JPY and EUR/JPY not only because they are indisputably closely related. They encompass the three most widely traded currencies but are also unique markets in themselves. The dataset includes snapshots of up to 10 levels of the order book for each currency pair. Level 1 is the highest and contains the best bid and ask prices; Level 2 is the second-highest, and so on. The time-slice interval is 100 milliseconds, and we use the price and volume at each depth of the limit order book.[1]

[1]Our methodology does not require an exceptionally detailed dataset. In fact, we make use of neither trader IDs nor transactions. Anonymity and the lack of trader IDs might appear problematic. However, data availability remains a major challenge not only for academic researchers, but also for surveillance departments. Traders and financial institutions have access to their own transactions and orders, but data on the behaviour of the rest of the market is typically heavily restricted in some form. Hence, we believe that the limit order book dataset in this study acts as a good representation.

3.2 Spoof Alerts

As described in Section 2, a spoof event can be decomposed into two parts: a spoof order (that is submitted and later cancelled) on one side and a genuine resting order on the other side of the order book. To construct proxies for what could constitute a spoof order, we use the 100-millisecond snapshots of the order volume for up to ten price levels on each side of the limit order book. The start of a spoof event always involves an order submission – an increase in the bid [ask] volume at a specific bid [ask] price. Conversely, the end of a spoof event involves an order cancellation – a decrease in the bid [ask] volume at the corresponding bid [ask] price. To recap, a spoof order is, by definition, intended to be cancelled. Thus, the change in the bid [ask] volume at specific bid [ask] price levels is central to generating the proxies. Going forward, we refer to these spoof order proxies as "spoof alerts".

More specifically, we identify all instances where the limit order volume at a particular price fits the footprint of a possible spoofing attempt by using five rules to identify a sequence of bid [ask] volumes $\{\text{volume}_t\}_{t=0}^{T} := \{\text{volume}_0, \ldots, \text{volume}_M, \ldots, \text{volume}_T\}$ all corresponding to the same price level P and satisfying:

1. All valid sequences contain a given snapshot M such that for all snapshots in the sequence before M, the sizes do not decrease between two consecutive snapshots: $\text{volume}_{t+1} - \text{volume}_t \geq 0 \; \forall t : 0 \leq t \leq M$.

2. For all snapshots after M, the sizez do not increase between two consecutive snapshots: $\text{volume}_{t+1} - \text{volume}_t \leq 0 \; \forall t : M \leq t \leq T$.

3. The final volume in the sequence is smaller or equal to the initial one: $\text{volume}_T \leq \text{volume}_0$.

4. The price P never reaches the first level of the limit order book during the sequence.

5. The price P never falls outside of the visible levels of the limit order book during the sequence.

(where t is the index of a particular snapshot in a particular limit order book). All sequences satisfying all five conditions are identified. Because each sequence involves one price, and each snapshot contains 18 such prices (9 on each side of the book, as the first level of the book is excluded from the sequence construction), it is possible to have up to

18 valid concurrent sequences at any given snapshot. The spoof alerts are described more formally in Section 4.1.

In order words, we assume that a spoof order, at no point in time, can be at the best bid [ask] price in the market or become "invisible" to the rest of the market (i.e. drop outside of the ten highest depth levels of the order book). This is logical, as a spoof order is neither intended to be executed (an immediate risk at the first level) nor perceived to have zero or minimal impact on the market (outside the visible limit order book). Furthermore, whereas we allow for one or several submissions at the same price, we always categorise a reduction in the order volume at the same price as the end of a spoof proxy.

Put differently, we permit spoofing strategies to increase in size gradually but require them to end immediately if there is even the slightest decrease. This is because spoofing strategies might involve several limit order submissions at the same price to increase the likelihood of a market reaction (similar to that of "layering", which could be classified as spoofing at multiple price levels). However, because a spoof order is never intended to be executed, there is no rational reason for a trader to gradually reduce spoof orders, regardless of whether the spoofing strategy has proven successful. For instance, in CFTC's charge against Skudder regarding spoofing the soybean derivatives market, the Commission found that the trader had cancelled more than 99% of spoof orders as part of the alleged single and cross-market spoofing schemes (CTFC, 2022).

Before we move on to the next phase of the methodology, let us briefly study the key characteristics of the spoof alerts that are generated. A summary for each currency pair is provided in Table 1.

As can be seen, the methodology generates 14-15 million spoof alerts per currency pair over the 17 months studied. However, it is important to remember that the huge number of alerts should not be interpreted as actual spoof orders. At this stage, we are only concerned with identifying any pattern inside the limit order book that might act as a building block toward a spoofing event.

The minimum limit order size on EBS is 1M USD or EUR, which is also the minimum spoof order quantity in million EUR or USD. The average is 1.80M, 2.14M and 1.45M for EUR/USD, USD/JPY and EUR/JPY, respectively. However, the maximum order quantities are 843M, 1,036M and 303M – demonstrating that the dataset also contains potential spoofs that are made up of large and/or many limit order submissions at the

same price. The minimum number of spoof order updates is 2 for all three currency pairs (consisting of 1 submission and 1 cancellation), whereas the maximum is 25, 30 and 14.

As noted earlier, we require spoof orders to range between Level 2 and Level 10 of the order book. The mean entry level is 4.11, 4.41 and 3.45 for EUR/USD, USD/JPY and EUR/JPY, respectively. The mean exit level is approximately the same. The distance to the best same side price is relatively similar for the three currency pairs: 1.6, 1.7 and 1.3 pips. The three FX spot markets are also highly competitive, as seen from the difference between the best opposite and same side prices. The mean bid-ask spreads are 1.0, 1.0 and 2.3 pips for EUR/USD, USD/JPY and EUR/JPY, respectively.[2]

The spoof lifetime measures the length of time (in seconds) between the first order submission in a spoofing sequence and the cancellation, which marks the end of that sequence. As can be seen from Table 1, the methodology generates spoof lifetimes that vary considerably. The average spoof lifetime is 14.3, 16.5 and 22.8 seconds for EUR/JPY EUR/USD, USD/JPY and EUR/JPY. However, the mean values are skewed due to a few spoofs being extremely long. The median is around 0.2 seconds - consistent with the notion that spoofing tactics could be more associated with algorithmic and high-frequency traders.

The total limit order book size (for the top-10 levels for the book) at the time of spoof entry is also an essential factor to account for. Everything else being equal, a spoof order is less likely to have an impact if the market is deep. Again, significant variations can be seen in Table 1. The mean limit order book size on the opposite side is approximately 80M, 74M and 27M for the three currency pairs. However, there are significant differences, with minimum [maximum] size being 1M [2,819M] for EUR/USD, 1M [2,225M] for USD/JPY and 1M [914M] for EUR/JPY. When viewed from the same side of the limit order book, the figures are approximately the same. Overall, it is notable from the above that all three markets covered in this study are extremely large, liquid and competitive. Nonetheless, EUR/JPY is quite far behind the top-2 currency pairs, consistent with being a cross (i.e. not involving the USD).

[2]Following the market convention, a "pip" refers the 5th decimal for EUR/USD, but the 3rd decimal for USD/JPY and EUR/JPY.

3.3 Market Reactions and Scenarios Compatible with Spoofing

A spoof order is not only intended to be cancelled. It is also intended to change the perception of supply and demand in the market and, as a result, trigger other traders to react in a certain way. When studying a limit order book as a whole, a successful spoof would ultimately result in a specific change in the best bid/ask price and/or the volume at the best bid/ask – stemming from the resting order at the first level having been executed. Spoofing itself does not require that a resting order becomes a profitable transaction for the trader. Some strategies might have no impact at all, or even the opposite impact of what was intended. If the timing is "unfortunate", the tactic might even generate a loss for the spoofer. In practice, however, surveillance departments and financial regulators would look for profitable transactions. In other words, they would try to "follow the breadcrumbs" as is common in financial crime investigations more generally.

It might seem logical to only study actual transactions for this process – and simply assume that some could have been genuine resting orders and part of a spoofing scheme. After all, a successful spoof involves a transaction at some point. However, this paper aims not to detect a particular case of spoofing or to identify the perpetrators. This is the job of surveillance departments and financial regulators. Instead, our emphasis lies on analysing the market reaction to differently calibrated spoof orders, and whether spoofing in one market also might have an impact on another market. Furthermore, on electronic trading platforms such as EBS, transactions account for only a minuscule fraction of activity (typically less than 1%) (Stenfors and Susai, 2019, 2021). Hence, we opt to utilise all volume and price data at the first level of the order book rather than transactions only.

The benefit of shifting the focus from the concept of transactions (or simply bid/ask prices) towards tradable volume at the bid/ask prices becomes clear if we deconstruct the potential changes to the first level of the limit order book between two snapshots (for a detailed discussion, see Stoikov, 2018). Table 2 shows that there are five possible reactions from the bid side (denoted B1 to B5) and five possible reactions from the ask side (A1 to A5).

This approach enables us to construct proxies for genuine resting orders that are executed but do not necessarily result in an immediate Level 1 price change (such as alternative B2). Further, it permits us to disregard market reactions that could be regarded as contradictory from a spoofing perspective (e.g. a combination of reaction B5

from the bid side and A5 from the ask side of the limit order book). It is also apparent that an empirical study only using price data would underestimate the frequency and granularity of market reactions. However, because we investigate the change between two 100-millisecond snapshots rather than two consecutive observations, both sides of the order books may have changed. Hence, we can differentiate between 25 mutually exclusive yet all-encompassing scenarios. Table 3 shows a summary.

Although the 25 scenarios are unique, dividing them into four categories makes sense.

Category 1 contains scenarios consistent with the market reaction to a successful spoof order. In scenarios 3, 4, 5, 8, 9 and 10, bid-side volume is withdrawn partially or entirely, whereas volume is added to the ask (i.e. offer) side or it remains unchanged. All these scenarios are compatible with a successful spoof from the ask-side of the limit order book. In scenarios 11, 12, 16, 17, 21 and 22, the ask-side volume is subject to a mirror-like market reaction. All these scenarios are compatible with a successful spoof from the bid-side of the limit order book.

Category 2 contains scenarios that could be considered as frontrunning. In scenarios 18 and 23, bid-side volume is added to the existing best price or an even better price, whereas the ask-side volume remains unchanged. For instance, we could conceptualise this as if a trader reacts to a large bid order submission at the second level of the book by submitting a more competitive order. In scenarios 14 and 15, ask-side volume is added to the existing best price or a better price, whereas the bid-side volume remains unchanged. None of these scenarios is compatible with a successful spoof.

Category 3 includes all instances where the market reaction is inconclusive. In scenarios 1, 2, 6, 7, 19, 20, 24 and 25, volume is either added to withdrawn from both sides of the limit order book between two snapshots. Consequently, the mid-price could either increase, decrease or remain unchanged – depending on the proportional change on both sides. None of these scenarios is compatible with a successful spoof.

Category 4 includes the unique scenario 13, where neither the bid nor the ask volume changes and, hence, the price remains unchanged. Again, this scenario is not compatible with a successful spoof.

Table 3 shows the proportion of the different scenarios for EUR/USD, USD/JPY and EUR/JPY from 1 October 2013 to 28 February 2015. There are between 38 and 41 million snapshots per currency pair during this period.[3]

[3]As outlined in Section 3, the time-slice interval is 100 milliseconds, so there could, in theory, be more

Category 1 includes the six scenarios consistent with successful ask-side spoofs (Scenario 3, 4, 5, 8, 9 and 10) and the six scenarios relating to bid-side spoofs (Scenario 11, 12, 16, 17, 21 and 22). Seen as two separate groups, these make up 14.3% and 14.3% for EUR/USD. The corresponding proportions are 13.7% and 14.0% for USD/JPY, and 11.4% and 11.5% for EUR/JPY.

Category 2 includes the two scenarios which are consistent with frontrunning from the ask side and the two from the bid side. Seen as separate groups, these make up 10.4% and 10.2% for EUR/USD. The corresponding proportions are 9.7% and 10.0% for USD/JPY, and 11.0% and 11.2% for EUR/JPY.

Category 3 contains scenarios 1, 2, 6, 7, 19, 20, 24 and 25. None of these mixed scenarios is compatible with a successful spoof. Notably, these are pretty rare and, when combined, only account for 2.7%, 2.7% and 1.5% for EUR/USD, USD/JPY and EUR/JPY, respectively.

Finally, we can see that 48.1% of all observations match Category 4 (Scenario 13) for EUR/USD. In this unique case, no change in volume is observed at Level 1 of the limit order book. The corresponding proportion for USD/JPY and EUR/JPY is 49.9% and 53.5%. Thus, roughly half of the snapshots involve some market reaction at the first level of the limit order book.

4 The Model and Results

4.1 Description Spoof Alert

Call $\text{Size}_t(\text{Price}, \text{Side}, \text{Date}, \text{Currency Pair}) := \text{Size}_t$ the time series of the posted sizes (bids or offers) in a given currency pair, date, side of the market and price. For example, Figure 1 depicts the values of Size_t for price 1.2465, Currency pair EUR/USD, Date 2014-12-14 and side "bid". The size values range from 1M to 11M. Before '20:05:47' that day, Size_t is 0 on the bid side of the book. From now on, to lighten the notation, we will omit the fixed arguments of Size_t so that, for example, Size_t and Size_T will denote the sizes on the same market, day, currency pair and side but at two different snapshots t and T). On a given day, we obtain Size_t for every price quoted that day.

observations (10x60x60x24x516=445,824,000). However, EBS does not generate a snapshot unless there is a trade or a change in the limit order book. Notably, too, there is no activity during weekends and holidays and also a thin market during the Pacific time zone.

For a given Price P, currency pair, date and side of the book, a spoof alert j is a subset of values of time indexes $t(j) = \{t_I(j), \ldots, t_M(j), \ldots, t_F(j)\}$ where $t_I(j), t_M(j), t_F(j)$ satisfy:

1. $\text{Size}_t - \text{Size}_{t-1} \geq 0$ for all $t \in \{t_I(j), \ldots, t_M(j)\}$: there exist an index $t_M(j)$ between $t_I(j)$ and $t_F(j)$ such that the Sizes are increasing to the left of $t_M(j)$ inside the alert unit.

2. $\text{Size}_t - \text{Size}_{t-1} \leq 0$ for all $t \in \{t_M(j) + 1, \ldots, t_F(j)\}$: there exist an index $t_M(j)$ between $t_I(j)$ and $t_F(j)$ such that the Sizes are deceasing to the right of $t_M(j)$ inside the alert unit.

3. $\text{Size}_{t_F(j)} \leq \text{Size}_{t_I(j)}$: at the end of the alert unit, the size get back at or below the value at the onset of the alert unit.

4. Price P never reaches the first level of the book during $t(j)$.

5. Price P never falls outside the visible book during $t(j)$.

Using the rules above, for a given Price P, currency pair, date and side of the book, the same time index t can be assigned to more than one spoof alert (consider, for example, the peak in size at 10M around 22:40 in Figure 1 which could be assigned to two nested spoof alerts). In such cases, we break the ties and consider only the innermost alert.

For a given Price, currency pair and side, on each spoof alert, we measure the following two variables:

Size:

$$\text{AddSize}_j = \log_2 \frac{\text{Size}_{t_M(j)} - \text{Size}_{t_I(j)}}{\sum_p \text{Size}_{t_I(j)}(p)} \tag{1}$$

For the j-th spoof alert, AddSize_j is the base 2 log of the ratio of the maximum size addition in the spoof alert to the total size of the order book on the same side as the order at the onset the spoof alert. The definition of the alert unit requires that $\text{Size}_{t_M(j)} > \text{Size}_{t_I(j)}$ always. Figure 3 depicts the distribution for the observations remaining after the matching described in Section 4.2. A large value indicates a sharp increase in posted size between the onset and the peak of the spoof alert. For example, the spoof alert around 21:40 in Figure 1 has peak size 8M, initial size 7M a total size on the bid side of the book of 32M and $\text{AddSize}_j = \log_2 \frac{8-7}{32}$.

Aggressiveness:

When side is bid:

$$\text{Agg}_j = -\log_2 \frac{\sum_{p>Price} \text{Size}_{t_I(j)}(p)}{\sum_{p\neq Price} \text{Size}_{t_I(j)}(p)} \tag{2}$$

When side is ask:

$$\text{Agg}_j = -\log_2 \frac{\sum_{p<Price} \text{Size}_{t_I(j)}(p)}{\sum_{p\neq Price} \text{Size}_{t_I(j)}(p)} \tag{3}$$

For the j-th spoof alert, Agg_j is the negative base 2 log of the size of all orders closer to the touch (i.e. the first level of the limit order book) at the onset of the spoof alert window, normalized by the size of all orders then present at all other levels of the same side of the book. For example, the spoof alert around 21:40 in Figure 1 has 20M worth of orders located at prices closer to the touch at time $t_I(j)$. The total size of the bid side of the order book at time $t_I(j)$ is 32M and the order itself has size 7M so that: $\text{Agg}_j = -\log_2 \frac{20}{32-7}$. This is a measure of Aggressiveness in that a large value corresponds to orders that are placed closer to the touch. Figure 2 shows the histogram of the values of Agg_j for the three markets. Note that by construction, Agg_j describes the configuration of the order book before the addition of $\text{Size}_{t_M(j)} - \text{Size}_{t_I(j)}$ so that Agg_j and AddSize_j are both driven by a common shock. This explains the absence of correlation between the two measures, which is visible from the plot of one against the other, shown in Figure 4.

Looking at Figures 2 and 3 we see that the values of Agg_j and AddSize_j largely overlap each other for the observations irrespective of currency pairs. Examining the uni-variate distributions closer through their respective histograms, the distribution of the values for EUR/JPY is less scattered than the dollar pairs. Going back to the construction of the variable, this means that spoof alerts obtained from EUR/JPY typically have lower peaks (compared to the total size of the half of the limit order book on which they sit) and is closer to the touch than those obtained from EUR/USD and USD/JPY.

Each spoof alert j is indexed by Side, Currency Pair, Price P, Date and time of $t_M(j)$, the time of maximum value of Size_t inside $t(j)$. To each spoof alert, we associate two numbers: Agg_j and AddSize_j as well as its side and currency pair.

4.2 Description Regression Design: Single-Market Spoofing Event

The purpose of this section is to quantify the relationship between shifts in internal book configuration at levels two and deeper and subsequent reaction in the configuration of the

top of the book for a given currency pair.

To each spoof alert, we associate the market reaction measurement nearest in time in the same market and on the same day that comes after it. Since the number of market reactions (124,330,290 when we consider all currency pairs, sides and dates combined but removing scenario 13, which corresponds to the "unchanged" outcome) is larger than the number of spoof alert events (44,772,965), it is possible for the same market reaction event to be associated to several spoof alerts. In those cases, for each such market reaction measurement, we break the ties by only keeping the match with the spoof alert nearest in time to the market reaction measurements. Considering all currency pairs, sides and dates combined, we end up with 20,662,224 observations after the tie breaks.

Figure 5 shows a histogram of the time spread (in 100ms) between spoof alert and market reaction. Positive values indicate that in the market reaction is taken on a snapshot strictly following the spoof alert peak time (a value of 8 indicates that 0.8 seconds have elapsed between the snapshot on which the peak size for the spoof alert was measured and the snapshot on which the market reaction was measured). Half the time, this spread is larger than 0. For the other half, the market reaction is measured at exactly the snapshot at which the size peaks for that alert unit.

When $Side_j$ (the side on which the spoof alert is measured) is bid, we fit Equation 4 on a response variable R_j that takes values 1 if market reaction matched with alert unit j is beneficial to a manipulator having submitted a resting order on the bid side of the book but spoofing from the opposite side (scenarios $\{3, 4, 5, 8, 9, 10\}$). Were $Side_j$ (the side on which the spoof alert is measured) is ask, we fit Equation 4 on a response variable R_j that takes values 1 if market reaction matched with spoof alert j is beneficial to a manipulator working a resting order on the ask side of the book but spoofing from the bid side (scenarios $\{11, 16, 21, 12, 17, 22\}$). For a given currency pair, we posit that the proportion of market reactions that are beneficial to a manipulator follows:

$$p_j = p(R_j = 1) = \left(1 + \exp\left(-\left(\alpha + \text{Agg}_j\beta_{\text{Agg}} + \text{AddSize}_j\beta_{\text{AddSize}}\right)\right)\right)^{-1} \tag{4}$$

The unconditional proportion of $R_j = 1$ in our sample is around 30% and the sample size around 7 million observations per currency pair. Fitting the logistic regression, we obtain the following coefficients (see table 4 for EUR/USD, table and table 6 for USD/JPY 5 for EUR/JPY.)

Several conclusion can be drawn from these tables.

Owing to the large sample size, all coefficients are statistically significant at any con-

ventional level, evincing that the variables Agg_j and AddSize_j have prediction power with respect to our measure of market outcome.

The share of explained variance is close to 1% in all cases, evincing that many other factors besides Agg_j and AddSize_j cause the observed market reaction.

The sign of the coefficients is consistent with a simple economic rationale: a would-be manipulator has to increase its execution risk (by increasing the size of his orders and putting those orders closer to the touch) to increase the probability of observing a desirable outcome in the subsequent snapshot. Thus, the manipulator faces a trade-off between execution risk and market impact - in line with the previous literature on FX order submission strategies (e.g. Lo and Sapp, 2010) and spoofing (Lee et al., 2013; Stenfors and Susai, 2021).

The coefficients are economically significant and all fairly similar (about 0.0725 for AddSize_j and 0.1 for Agg_j irrespective of side or currency pair). For example, for EUR/USD, a spoofer increases the probability of observing a desirable outcome in the subsequent snapshot by 5% for each doubling of Size at a given price. Likewise (still using EUR/USD as example), all other things equal, each halving of the size in front of the manipulator's order at the onset causes a 6.5% increase in the probability of observing a desirable outcome in the subsequent snapshot. For example, consider now a spoof attack on the second level of the bid side of the limit order book of the EUR/USD market that causes Agg_j and AddSize_j to move from their mean values[4] to 7 and -2.7, respectively. This happens for example if the total size of the bid side of the limit order book in EUR/USD is 130M (the 95 percentile of the total size of the bid book in this market in our sample if 135 million), the size at the top of the bid side is 1M (before the spoof action) and the participant adds 20M to the second level of the book[5]. These values that fall within the top 1% of historical experience for Level 2 of the limit order book in the EUR/USD market in our sample, meaning that we observe them over one hundred times on a typical day. According to our fitted model, an addition of this magnitude increases in the probability of observing a favourable outcome (i.e. a successful spoof) at the next snapshot from about 33% to 44%, an economically significant difference.

[4]The average value of Agg_j on the EUR/USD market is 4.55 in our sample. The average value of Agg_j for orders posted on the second level of the order book is -5.42.

[5]Assuming that before the spoof action, the second level of the book had already 5M worth of orders on it, had the 20M order been a 3M order posted on the third level of the book, the values of $\text{Agg}_j = -\log 2\frac{6}{130} \approx 4.5$ and $\text{AddSize}_j = \log 2\frac{3}{130} \approx -5.5$ would be close to their respective averages.

4.3 Description Regression Design: Cross-Market Spoofing Event

Now consider a case whereby a trader submits a genuine resting order in one market but submits a spoof order in a closely related market instead. Thus, the purpose of this section is to quantify the relationship between shifts in the internal book configuration at levels two and deeper in a given currency pair and subsequent reaction in the configuration of the top of the book for another currency pair.

Because all markets we use are related (they each share a currency with the other two), the configuration in the limit order book of one market – and changes thereof – is likely to spill over to the others. Therefore, the relationship between the characteristics of the spoof alerts in a given market X and the nature of subsequent market reaction in a currency pair Y has to account for the characteristics of the effect of the contemporaneous spoof alert in currency Y in the specification as well.

As before, we index (or locate in time) each spoof alert at the time at which the size reaches its maximum value and match this with the timestamp in which the market reaction is measured. More specifically, consider three markets, X, Y and Z. Each spoof alert is indexed by the time at which the peak size is attained ($t^x_M(j)$ for market X, $t^y_M(j)$ for market Y, $t^z_M(j)$ for market Y). To each spoof alert on X, we associate the market reaction measurement nearest in time that comes after it in market Y. We do the same for market Z and Y. Note that in the case of market Y we use the same market to locate the maximum value and the market reaction. It still holds that the number of market reactions is larger than the number of spoof alert events and, as before, it is possible for the same market reaction event to be associated with several alerts. In those cases, for each such market reaction measurement, we again break the ties by only keeping the match with the spoof alert nearest in time for each market. To include all three markets in the same regression, we use only those matched market reaction snapshots common to all three markets. This strategy minimizes the risk of measurement biases but also greatly reduces our sample size. Considering all possible currency pairs, sides and dates combined, we now have 1,829,123 data points in our regressions or about 10% of the observation count of the single-market regressions of Section 4.2.

The loss in terms of the effective number of observations used in each regression is better gauged by looking at the increased difference between, on the one hand, the time in which the earliest of the two spoof alerts happens and, on the other, the market reaction time. The more observations we lose compared to the single-market design (as a result

of the matching process), the greater this time spread will be. Consider the scatter of the histogram of these time differences, which is shown in Figure 7. The scatter is now larger than that shown in Figure 5. The time spreads between the first alert unit and the response time is now strictly positive 70% of the time (versus 50% in the first specification). The greater separation between the time in which the left hand and the right-hand side of our regression, *in fine*, causes a decrease in the accuracy of the estimated coefficient through an increase in the proportion of unexplained variance.

Whenever either the first or second currency X or Y pairs is the same, when $Side_j^y$ (the side on which the alert unit is measured on currency pair Y) and $Side_j^x$ (the side on which the spoof alert is measured on currency pair X) are bid, we fit Equation 5 on a response variable R_j^y that takes values 1 if market reaction matched with spoof alert j is beneficial to a manipulator working on the bid side of the book (scenarios $\{3, 4, 5, 8, 9, 10\}$). Whenever neither the first nor the second currency in the pairs X or Y is the same, when $Side_j^y$ (the side on which the spoof alert is measured on currency pair Y) is bid and $Side_j^x$ (the side on which the spoof alert is measured on currency pair X) is offer, we fit Equation 5 on a response variable R_j that takes values 1 if market reaction matched with spoof alert j is beneficial to a manipulator working on the bid side of the book (scenarios $\{3, 4, 5, 8, 9, 10\}$). The same logic applies straightforwardly when $Side_j^y$ is offer (and $Side_j^x$ is bid or offer depending on whether either the first or second currency in X and Y are the same or not) and when considering the the Z market in relation, again, to the Y market. For a given currency pair, we posit that the proportion of market reactions that are beneficial to a manipulator follows:

$$\begin{aligned} p_j = p(R_j^y = 1) = \big(1 + \exp\big(-\big(\alpha + \mathrm{Agg}_j^x \beta_{\mathrm{Agg}}^x + \mathrm{AddSize}_j^x \beta_{\mathrm{AddSize}}^x + \\ \mathrm{Agg}_j^y \beta_{\mathrm{Agg}}^y + \mathrm{AddSize}_j^y \beta_{\mathrm{AddSize}}^y + \\ \mathrm{Agg}_j^z \beta_{\mathrm{Agg}}^z + \mathrm{AddSize}_j^z \beta_{\mathrm{AddSize}}^z\big)\big)^{-1} \end{aligned} \tag{5}$$

The variables β_{Agg}^x, $\beta_{\mathrm{AddSize}}^x$, β_{Agg}^z and $\beta_{\mathrm{AddSize}}^z$ are now the main coefficients of interest. As explained above, the variables $\mathrm{AddSize}_j^y$ and Agg_j^y are included to control for the effect of the limit order book dynamic in currency Y itself which, if omitted, would bias the coefficients of interest away from 0.

The unconditional proportion of $R_j^y = 1$ in our sample is around 30%. Fitting the logistic regression, we obtain the following coefficients (see Table 7 for EUR/USD, Table 8 for USD/JPY and Table 9 for EUR/JPY.)

The coefficients $\beta^{y}_{\text{AddSize}}$ and β^{y}_{Agg}, which measure the effect a change in the limit order book has in the same market (the endogenous effect of size and aggressiveness) are of comparable magnitude to those of Section 4.2, although the coefficients of AddSize_j in the cross-market specifications are always a bit smaller than their counterpart from the single-market specification.

The coefficients associated with the effect of the change in the other currency pair (the exogenous impact of changes in the book structure of currency pair X and Z on currency pair Y) are always smaller than the endogenous ones. However, the extent depends on whether the exogenous currency pair is a cross (EUR/JPY) or dollar-based. When the endogenous market is either EUR/USD or USD/JPY, the coefficients of the exogenous market tend to be smaller, at about one half of the effect size (although they are mostly still statistically significant). Changes inside the USD/JPY order book seem to have a more substantial impact on the subsequent Level 1 reaction for EUR/USD than the other way around. Looking at the cross (EUR/JPY), we see that it is the one for which the coefficients associated with the exogenous changes are the largest, in all cases significant and greater than half of the coefficients related to the endogenous effect. This suggests that a reliable pathway exists that a manipulator can exploit: to post genuine buy [sell] resting orders in the EUR/JPY market and then submit spoof sell [buy] orders in the EUR/USD or USD/JPY market.

4.4 Robustness Checks

In this work, we tried several specifications for measuring the size and aggressiveness of a spoof alert. In this section, we review the main candidates.

The variable AddSize accounts for the increase in size at a price level from the onset of a spoof alert to its maximum value inside the alert. An alternative, simpler specification, would be:

$$\text{AddSizeAlt}_j = \log_2 \frac{\text{Size}_{t_M(j)}}{\text{Size}_{t_I(j)}} \tag{6}$$

Figure 6 shows the distribution of the values of AddSizeAlt_j for the three markets. The distribution of AddSizeAlt_j is very clumped for EUR/JPY –with the majority of the observations taking values $\frac{\text{Size}_{t_M(j)}}{\text{Size}_{t_I(j)}} \in \{0.5, 2, 3\}$. The concentration at a handful of values of AddSizeAlt for one of the currency pairs renders the interpretation of the coefficients in regression model (in terms of changes in outcome in response to marginal changes in AddSizeAlt) as well as the comparison of the coefficients between the currency pairs

more difficult. The raw size numbers are also heavily impacted by the patterns of market activity (order sizes are bigger at some times of the day or on some dates with important events). Normalising by the total size of the half of the book in which the order is posted (bid side of the book if the numerator is on the bid side) as we do for AddSize yields a more spread out set of values for all currency pairs as shown in Figure 3. Normalising also neutralises out the component of the order sizes that are due to the general ebb and flow in overall market activity, which are not germane to our focus here.

The variable Agg accounts for how close an order is placed to the top of the book. Orders placed close to the top of the book convey greater urgency. As they are more likely to get hit, they play a greater role in the price discovery process and are thus more likely to impact the behaviour of other market participants. The natural way to measure how close an order is to the top of the order book is by looking at the level at which it is posted. However, this measure is very clumpy, making the interpretation in terms renders the interpretation of the coefficients in the regression model (as changes in outcome in response to marginal changes in AddSizeAlt) inapplicable.

5 Conclusions

In this paper, we empirically explore the feasibility of cross-market spoofing – and hence its potential prevalence in global financial markets. To do so, we use an EBS FX spot dataset covering the period from 1 October 2013 to 31 February 2015. As a pilot study, we have chosen three currency pairs (EUR/USD, USD/JPY and EUR/JPY) that are not only unique markets but also indisputably closely related. More specifically, we first construct a model that generates approximately 44 million spoof alerts. These correspond to patterns of submissions and cancellations within the limit order book that, when seen from the perspective of other market participants, could be seen as potential spoofs. We then study the change at the first level of the order book at 100-millisecond intervals and categorise 124 million market reactions into 25 mutually exclusive yet all-encompassing scenarios. Next, we match the spoof alerts with the market reaction nearest in time and end up with 20,662,224 observations. Finally, we run models that quantify the relationship between shifts in the internal book configuration between Levels 2 and 10 of the order book (outside the best bid/ask yet visible to other market participants) and the subsequent reaction at the top of the book. Using measurements for size and aggressiveness, we test

the impact from both sides of the order book and from both a single and cross-market perspective. The single-market results show that predictable reactions follow potential spoofs (endogenous to the market in question) that a market manipulator may exploit. In other words, it increases the likelihood of filling a genuine resting order. The results are statistically and economically significant. The cross-market results indicate that when the endogenous market is either EUR/USD or USD/JPY, the coefficients of the exogenous markets tend to be smaller. However, we find that EUR/JPY offers a reliable pathway for a manipulator to exploit via spoof orders at deeper levels in the EUR/USD or USD/JPY limit order books. Overall, our pilot study lends support to the increasing attention to cross-market manipulation by compliance officers and financial regulators.

Figure 1: Bid size at the price 1.2465 for EUR/USD on 2014-12-14. Source: EBS.

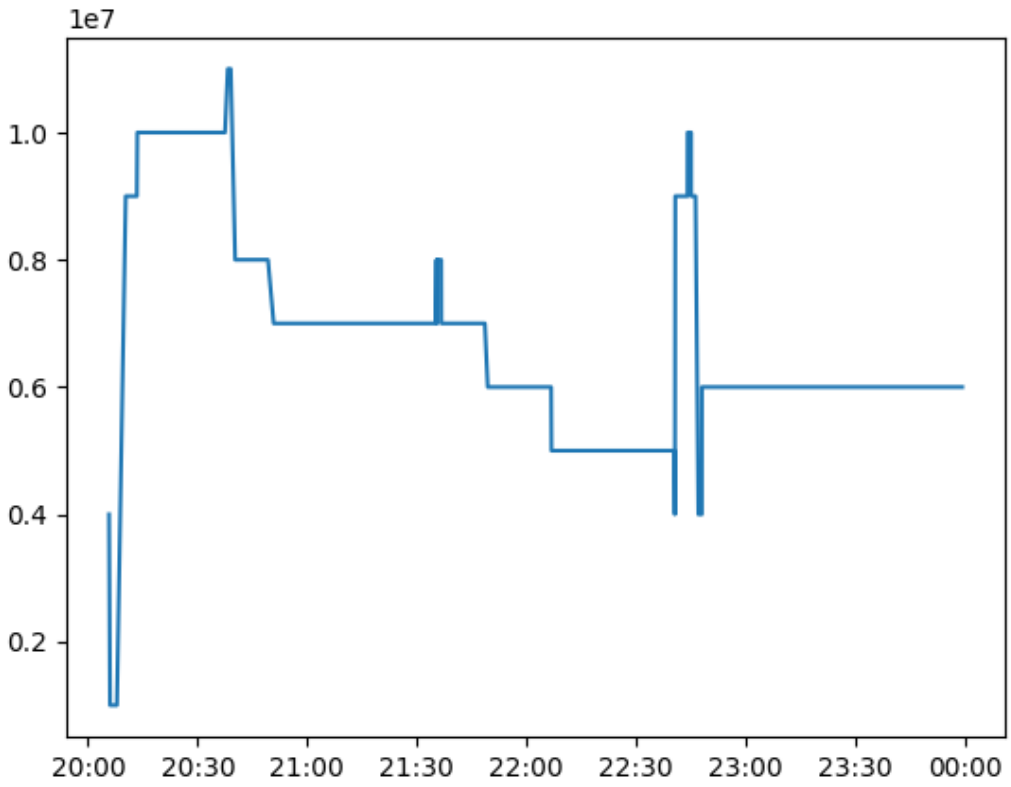


Table 1: Spoof alerts – Summary statistics.

Characteristic	Statistic	EUR/USD	USD/JPY	EUR/JPY
Number of spoof alerts	Total	14,313,215	15,726,394	14,733,356
Spoof quantity (volume in M)	Mean	1.80	2.14	1.45
	Median	1.00	1.00	1.00
	Min	1.00	1.00	1.00
	Max	843.00	1,036.00	303.00
Spoof quantity (number of order updates)	Mean	2.40	2.41	2.26
	Median	2	2	2
	Min	2	2	2
	Max	25	30	14
Entry level	Mean	4.11	4.41	3.45
	Median	3	3	3
	Min	2	2	2
	Max	10	9	10
Exit level	Mean	4.09	4.42	3.46
	Median	3	3	3
	Min	2	2	2
	Max	10	10	10
Distance to first level at entry	Mean	0.00016	0.01725	0.01355
	Median	0.00010	0.01000	0.01000
Bid-ask spread at entry	Mean	0.00010	0.01039	0.02335
	Median	0.00010	0.01500	0.02500
Spoof lifetime (seconds)	Mean	14.3	16.5	22.8
	Median	0.2	0.2	0.2
	Min	0.0	0.0	0.0
	Max	68,673.5	78,198.1	71,004.4
Opposite-side LOB size at entry (M)	Mean	79.88	74.06	26.78
	Median	72.00	62.00	26.00
	Min	1.00	1.00	1.00
	Max	2,819.00	2,225.00	914.00
Same-side LOB size at entry (M)	Mean	77.89	72.96	25.64
	Median	71.00	61.00	25.00
	Min	3.00	3.00	3.00
	Max	2,826.00	2,221.00	734.00

Table 2: Alternative reactions

Reaction	Explanation
$[B1]$	Bid-side volume hit or withdrawn completely
$[B2]$	Bid-side volume hit or withdrawn partially
$[B3]$	Bid-side volume unchanged
$[B4]$	Bid-side volume added to the existing best price
$[B5]$	Bid-side volume added at a better price
$[A1]$	Ask-side volume hit or withdrawn completely
$[A2]$	Ask-side volume hit or withdrawn partially
$[A3]$	Ask-side volume unchanged
$[A4]$	Ask-side volume added to the existing best price
$[A5]$	Ask-side volume added at a better price

Figure 2: Distribution of Agg_j for the observations remaining after the matching described in Section 4.2 (all currency pairs, sides and dates combined). USD/JPY is in dark blue, EUR/USD in purple and EUR/JPY in green. Source: EBS and authors' calculations.

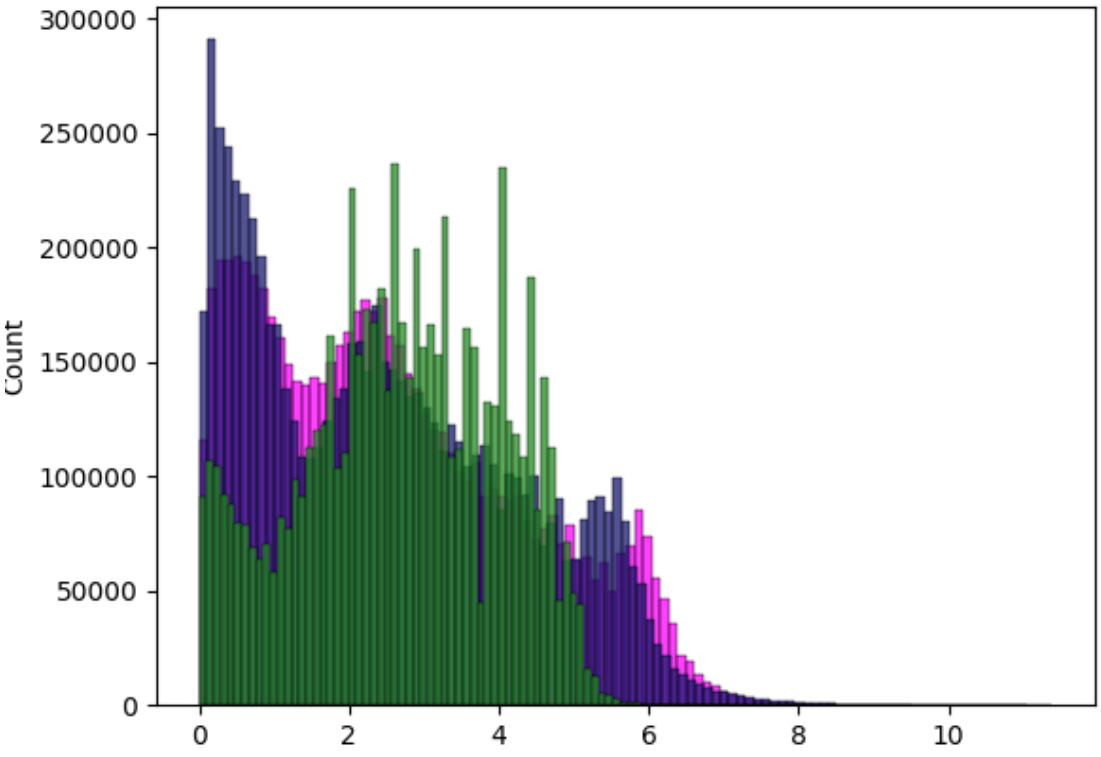


Table 3: Market reactions and scenarios

Currency pair			EUR/USD	USD/JPY	EUR/JPY
Number of snapshots			38,715,949	44,185,244	41,429,097
Scenario	Combination	Category	Proportion	Proportion	Proportion
1	$[B1]$ $[A1]$	Mixed	0.1%	0.1%	0.1%
2	$[B1]$ $[A2]$	Mixed	0.3%	0.3%	0.1%
3	$[B1]$ $[A3]$	Spoof	2.6%	2.5%	3.3%
4	$[B1]$ $[A4]$	Spoof	0.9%	0.9%	0.5%
5	$[B1]$ $[A5]$	Spoof	1.0%	1.0%	0.9%
6	$[B2]$ $[A1]$	Mixed	0.4%	0.3%	0.1%
7	$[B2]$ $[A2]$	Mixed	0.6%	0.6%	0.2%
8	$[B2]$ $[A3]$	Spoof	7.1%	6.7%	5.2%
9	$[B2]$ $[A4]$	Spoof	1.8%	1.8%	0.7%
10	$[B2]$ $[A5]$	Spoof	0.9%	0.9%	0.6%
11	$[B3]$ $[A1]$	Spoof	2.6%	2.5%	3.5%
12	$[B3]$ $[A2]$	Spoof	7.1%	6.9%	5.3%
13	$[B3]$ $[A3]$	Unchanged	48.1%	49.9%	53.5%
14	$[B3]$ $[A4]$	Front running	7.8%	7.8%	7.1%
15	$[B3]$ $[A5]$	Front running	2.4%	2.2%	4.1%
16	$[B4]$ $[A1]$	Spoof	0.9%	0.9%	0.5%
17	$[B4]$ $[A2]$	Spoof	1.8%	1.8%	0.7%
18	$[B4]$ $[A3]$	Front running	7.9%	7.5%	6.9%
19	$[B4]$ $[A4]$	Mixed	0.6%	0.8%	0.5%
20	$[B4]$ $[A5]$	Mixed	0.2%	0.3%	0.2%
21	$[B5]$ $[A1]$	Spoof	1.0%	1.0%	0.9%
22	$[B5]$ $[A2]$	Spoof	0.9%	0.9%	0.6%
23	$[B5]$ $[A3]$	Front running	2.4%	2.2%	4.0%
24	$[B5]$ $[A4]$	Mixed	0.2%	0.3%	0.2%
25	$[B5]$ $[A5]$	Mixed	0.1%	0.1%	0.1%
Total			100.0%	100.0%	100.0%

Table 4: Fitted single-market coefficients for EUR/USD, n = 6,790,346.

Coef.	Value	Std. Error	t-stat.
α	-0.764	0.005	.
β_{AddSize}	0.073***	0.001	83
β_{Agg}	0.1***	<0.001	210

Table 5: Fitted single-market coefficients for EUR/JPY, n = 6,678,613.

Coef.	Value	Std. Error	t-stat.
α	-1.142	0.005	.
β_{AddSize}	0.036***	0.001	30
β_{Agg}	0.11***	0.001	160

Table 6: Fitted single-market coefficients for USD/JPY, n = 7,193,265.

Coef.	Value	Std. Error	t-stat.
α	-0.721	0.004	.
β_{AddSize}	0.084***	0.001	107
β_{Agg}	0.115***	<0.001	253

Table 7: Fitted cross-market coefficients when the market Y is EUR/USD, market x is EUR/JPY and market z is USD/JPY. Sample size is n = 678,741.

Coef.	Value	Std. Error	t-stat.
α	-0.6425	0.027	.
β^x_{AddSize}	0.038***	0.004	9
β^x_{Agg}	0.002	0.002	<2
β^y_{AddSize}	0.049***	0.003	16
β^y_{Agg}	0.08***	0.002	48
β^z_{AddSize}	0.035***	0.003	12
β^z_{Agg}	0.044***	0.002	26

Table 8: Fitted cross-market coefficients when market Y is USD/JPY, market x is EUR/USD and market z is EUR/JPY. Sample size is n = 580,017.

Coef.	Value	Std. Error	t-stat.
α	-0.788	0.027	.
β^x_{AddSize}	0.0013	0.003	<2
β^x_{Agg}	0.0275***	0.002	17
β^y_{AddSize}	0.066***	0.003	24
β^y_{Agg}	0.11***	0.002	65
β^z_{AddSize}	0.039***	0.004	10
β^z_{Agg}	0.036***	0.002	16

Table 9: Fitted cross-market coefficients when market Y is EUR/JPY, market x is EUR/USD and market z is USD/JPY. Sample size is n = 678,741

Coef.	Value	Std. Error	t-stat.
α	-0.925	0.025	.
β^x_{AddSize}	0.018***	0.003	6
β^x_{Agg}	0.051***	0.002	33
β^y_{AddSize}	0.034***	0.004	9
β^y_{Agg}	0.08***	0.002	36
β^z_{AddSize}	0.039***	0.003	15
β^z_{Agg}	0.072***	0.002	48

Figure 3: Distribution of AddSize_j for the observations remaining after the matching described in Section 4.2 (all currency pairs, sides and dates combined). USD/JPY is in dark blue, EUR/USD in purple and EUR/JPY in green. Source: EBS and authors' calculations.

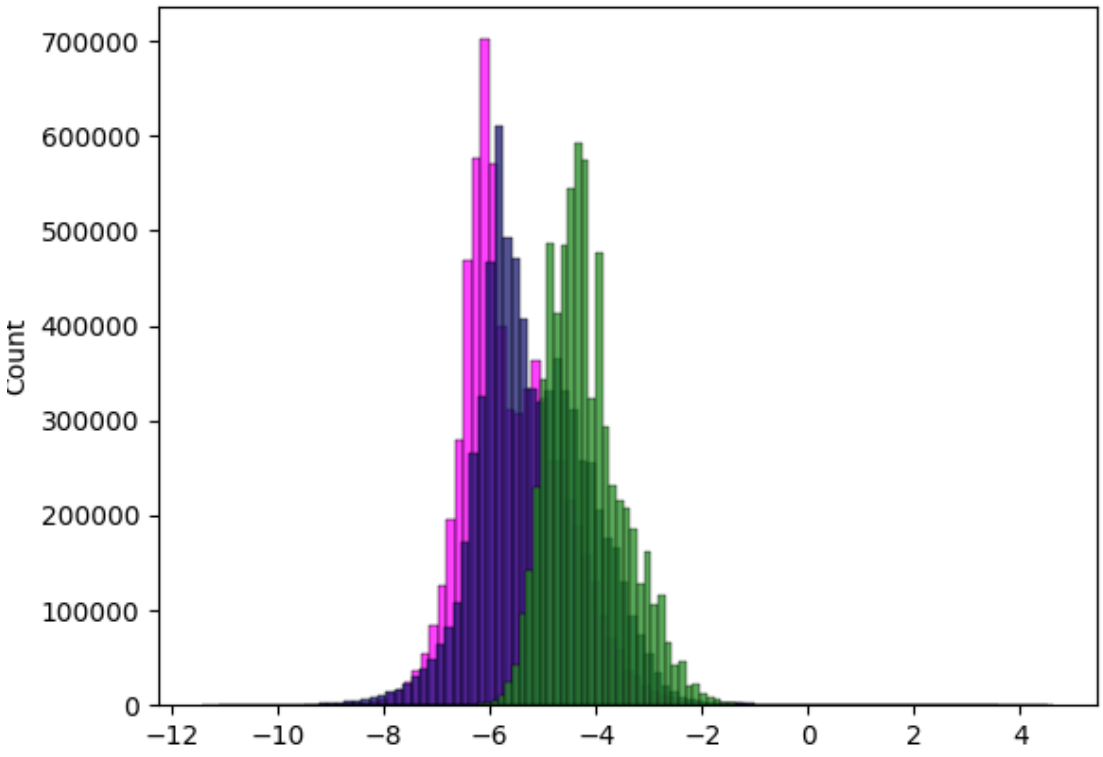


Figure 4: Scatterplot of AddSize_j against Agg_j for the observations remaining after the matching described in Section 4.2 (all currency pairs, sides and dates combined). USD/JPY is in dark blue, EUR/USD in purple and EUR/JPY in green. Source: EBS and authors' calculations.

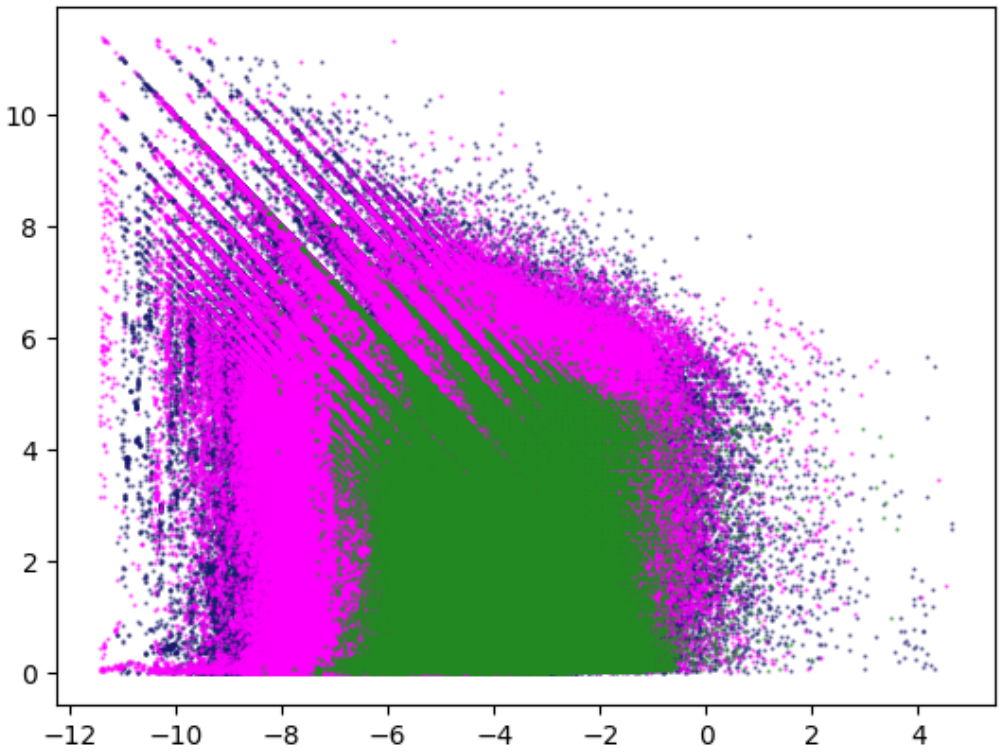


Figure 5: Distribution of time differences (in 100ms) between $t_M(j)$ (for all three markets combined) and the time of the nearest market reaction measurement after the matching described in Section 4.2 (all currency pairs, sides and dates combined). Source: EBS and authors' calculations.

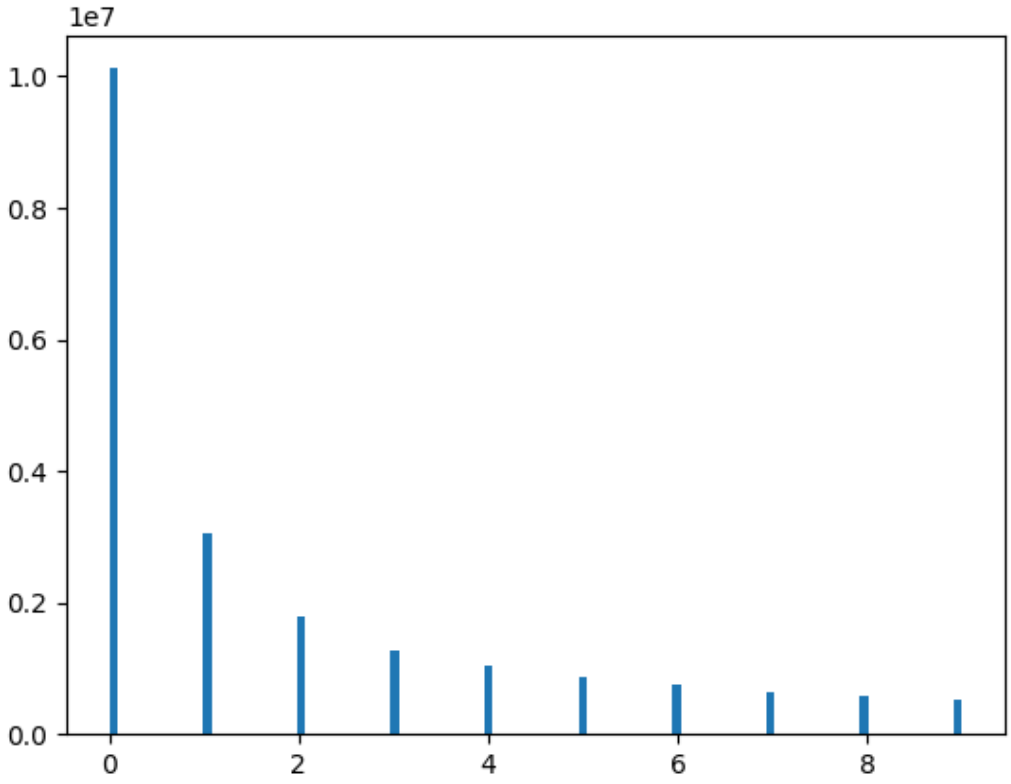


Figure 6: Distribution of the values of AddSizeAlt_j for the observations remaining after the matching described in Section 4.2 (all currency pairs, sides and dates combined). USD/JPY is in dark blue, EUR/USD in purple and EUR/JPY in green. Source: EBS and authors' calculations.

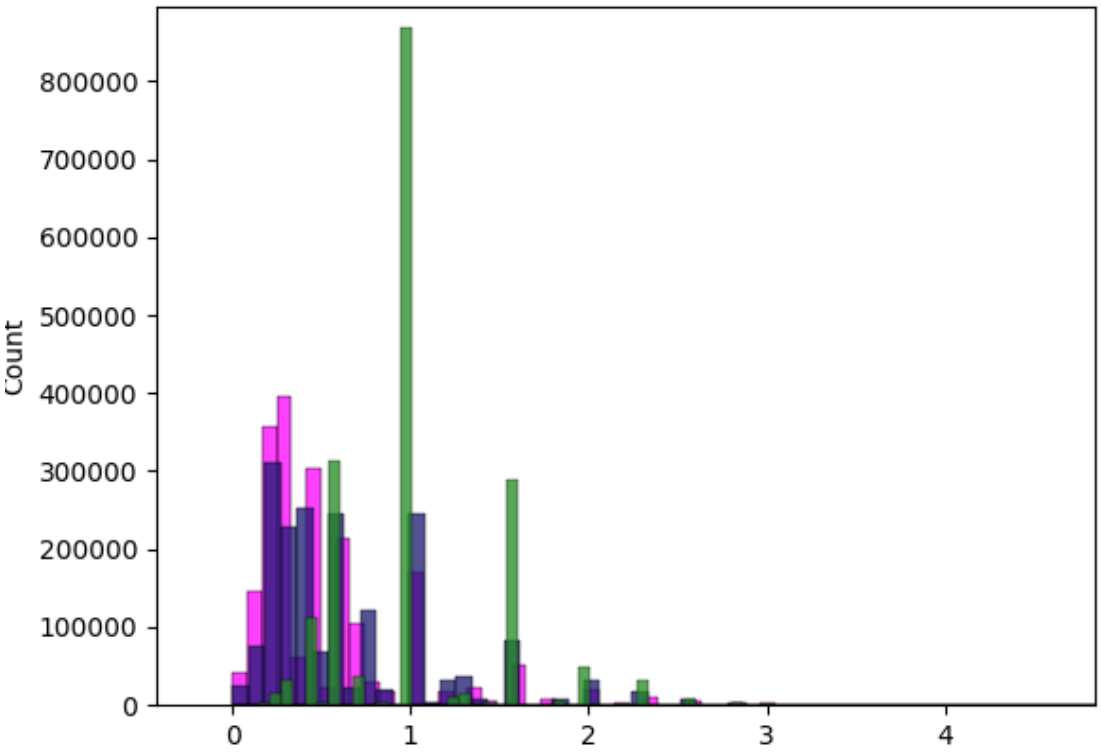
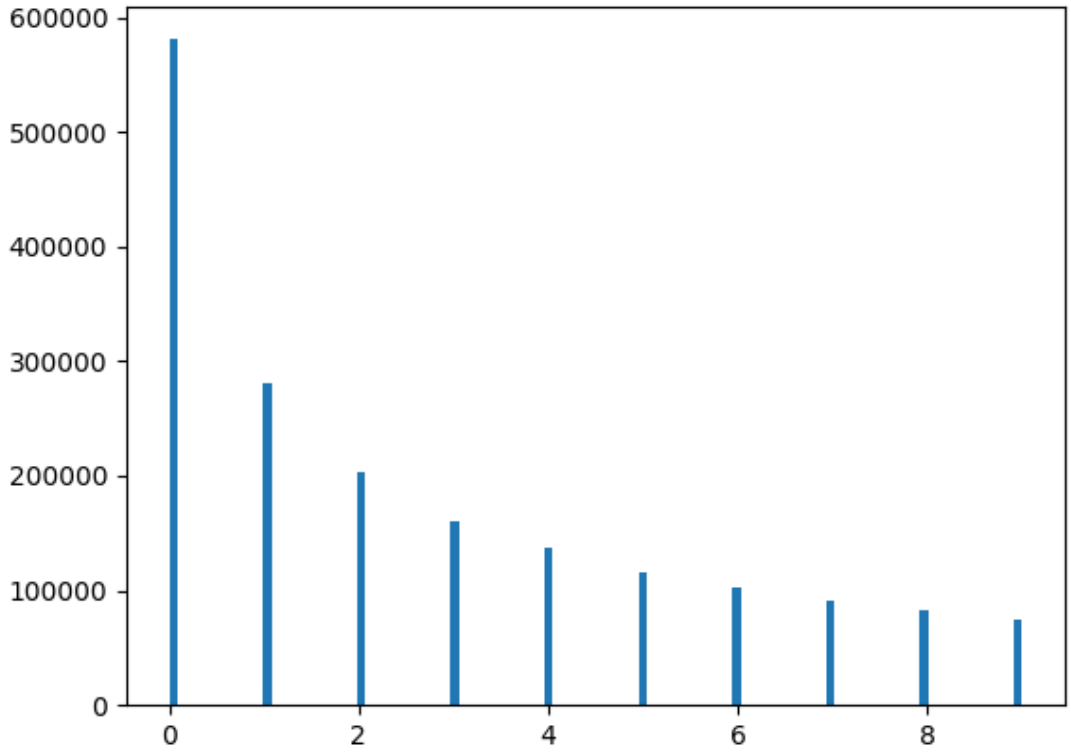


Figure 7: Distribution of time differences (in 100ms) between $t_M(j)$ (for all three 3 markets combined) and the time of the nearest subsequent market reaction measurement after the matching described in Section 4.3 (all currency pairs, sides and dates combined). Source: EBS and authors' calculations.



References

[1] AMF, 2019. The Enforcement Committee of the Autorité des Marchés Financiers fines Morgan Stanley & Co International Plc for manipulating the price of sovereign bonds and a sovereign bond futures contract, 10 December. Available from: https://www.amf-france.org/en/news-publications/news-releases/enforcement-committee-news-releases/enforcement-committee-autorite-des-marches-financiers-fines-morgan-stanley-co-international-plc [accessed 18 April 2022].

[2] CFTC, 2018. CFTC Files Eight Anti-Spoofing Enforcement Actions against Three Banks (Deutsche Bank, HSBC UBS) Six Individuals, 29 January. Available from: http://www.cftc.gov/PressRoom/PressReleases/pr7681-18 [accessed 18 April 2022].

[3] CFTC, 2020. CFTC Orders JPMorgan to Pay Record $920 Million for Spoofing and Manipulation, 29 September. Available from: https://www.cftc.gov/PressRoom/PressReleases/8260-20 [accessed 18 April 2022].

[4] CFTC, 2022. CFTC Charges Tennessee Trader and Two Entities with Engaging in Cross-Market and Single-Market Spoofing and Manipulative Schemes, 14 April. Available from: https://www.cftc.gov/PressRoom/PressReleases/8514-22 [accessed 22 April 2022].

[5] Chatziantoniou, I., Gabauer, D., Stenfors, A., 2020. From CIP-Deviations to a Market for Risk Premia: A Dynamic Investigation of Cross-Currency Basis Swaps. Journal of International Financial Markets, Institutions Money, 69, 101245.

[6] Chatziantoniou, I., Gabauer, D., Stenfors, A., 2021. Interest Rate Swaps and the Transmission Mechanism of Monetary Policy: A Quantile Connectedness Approach. Economics Letters, 204, 109891.

[7] Cumming, D., Dannhauser, R., Johan, S., 2015. Financial market misconduct and agency conflicts: A synthesis and future directions. Journal of Corporate Finance, 34, 150–168.

[8] Cumming, D., Johan, S., Li, D., 2011. Exchange trading rules and stock market liquidity. Journal of Financial Economics, 99, 651–671.

[9] Daníelsson , J., Luo, J., Payne, R., 2012. Exchange rate determination and inter-market order flow effects. European Journal of Finance, 18 (9), 823–840.

[10] DOJ, 2021. NatWest Markets Pleads Guilty to Fraud in U.S. Treasury Markets, 21 December. Available from: https://www.justice.gov/opa/pr/natwest-markets-pleads-guilty-fraud-us-treasury-markets [accessed 21 April 2022].

[11] FCA, 2010. Final Notice: Andrew Charles Kerr, 1 June. Available from: https://www.fca.org.uk/publication/final-notices/andrew-kerr.pdf [accessed 21 April 2022].

[12] FCA, 2012. Final Notice: UBS AG, 19 December. Available from: https://www.fca.org.uk/publication/final-notices/ubs.pdf [accessed 22 April 2022].

[13] FCA, 2014. Final Notice: Mark Stevenson, 20 March. Available from: https://www.fca.org.uk/publication/final-notices/mark-stevenson.pdf [accessed 18 April 2022].

[14] FCA, 2018. Market Watch 56, September. Available from : https://www.fca.org.uk/publication/newsletters/market-watch-56.pdf [accessed 21 April 2022].

[15] Financial Services Agency, 2019. Administrative Actions against Citigroup Global Markets Japan Inc., 7 June. Available from: https://www.fsa.go.jp/en/news/2019/20190607-2.html [accessed 18 April 2022].

[16] Fong, K. Y. L., Liu, W. M., 2010. Limit order revisions. Journal of Banking and Finance, 34, 1873–1885.

[17] Fox, M. B., Glosten, L. R., Guan, S. S., 2021. Spoofing and Its Regulation. Columbia Business Law Review, 2021 (3), 1244-1320.

[18] Gideon, M., 2019. Spoofing and Layering. Journal of Corporation Law, 45 (2), 101-169.

[19] Ilmanen, A., 1995. Time-Varying Expected Returns in International Bond Markets. The Journal of Finance, 50 (2), 481-506.

[20] Jotikasthira, C., Le, A., Lundblad, C., 2015. Why do term structures in different currencies co-move? Journal of Financial Economics, 115 (1), 58-83.

[21] King, M. R., Rime, D., 2010. The $4 trillion question: what explains FX growth since the 2007 survey? BIS Quarterly Review, December 2010.

[22] Lee, E. J., Eom, K. S., Park, K. S., 2013. Microstructure-based manipulation: Strategic behaviour and performance of spoofing traders. Journal of Financial Markets, 16, 227–252.

[23] Liu, W-M., 2009. Monitoring and limit order submission risks. Journal of Financial Markets, 12, 107–141.

[24] Lo, I., Sapp, S. G., 2010. Order Aggressiveness and Quantity: How Are They Determined in a Limit Order Market? Journal of International Financial Markets, Institutions and Money, 20, 213-237.

[25] Nasdaq, 2019. 2019 Nasdaq Global Compliance Survey. Available from: https://www.nasdaq.com/2019-Global-Compliance-Survey [accessed 21 April 2022].

[26] Nasdaq, 2022. Spoofing in Fixed Income Markets: What Does it Look Like?, 3 February. Available from: https://www.nasdaq.com/articles/spoofing-in-fixed-income-markets%3A-what-does-it-look-like [accessed 21 April 2022].

[27] Pirrong, C., 2017. The economics of commodity market manipulation: A survey. Journal of Commodity Markets, 5, 1–17.

[28] Securities and Exchange Surveillance Commission, 2018. Recommendation for Administrative Monetary Penalty Payment Order for Market Manipulation of 10-year Japanese Government Bond Futures by Mitsubishi UFJ Morgan Stanley Securities Co., Ltd., 29 June. Available from:

https://www.fsa.go.jp/sesc/english/news/reco/20180629.html [accessed 18 April 2022].

[29] Stenfors, A., 2020. Manipulative and Collusive Practices in FX Markets, in Cumming, D. and Alexander, C. (eds.) The Handbook of Fraud, Misconduct and Manipulation in Financial Markets. Hoboken, NJ: John Wiley Sons.

[30] Stenfors, A., Susai, M., 2019. Liquidity Withdrawal in the FX Spot Market: A Cross-Country Study Using High-Frequency Data. Journal of International Financial Markets, Institutions and Money, 59, 36–57.

[31] Stenfors, A. and Susai, M., 2021. Spoofing and Pinging in Foreign Exchange Markets. Journal of International Financial Markets, Institutions and Money, 70, 101278.

[32] Stoikov, S., 2018. The micro-price: a high-frequency estimator of future prices. Quantitative Finance, 18 (12), 1959-1966.

[33] Sutton, G. D., 2000. Is there excess comovement of bond yields between countries? Journal of International Money and Finance, 19 (3), 363-376.