Can Machine Learning in Finance Inform Clinical Decision Support?

Published on December 12, 2019

Scott W. Bauguess

Director, Program on Financial Markets Regulation, McCombs School of Business

AMIA KEYNOTE ADDRESS

Thank you, Jeff [Smith] for the introduction, and also for the invitation to speak here today, at the AMIA 2019 Health Informatics Policy Forum. It feels good to be back in DC. I joined the University of Texas in September, and I'm still getting used to my transition from federal government. This includes speaking in my private capacity as a professor. It was usually at this point in my previous public remarks as a securities markets regulator that I gave a disclaimer – that my views do not necessarily reflect the views of the Securities and Exchange Commission. While that is no longer necessary, I do feel compelled to make a disclaimer: my remarks today may at times not be directly applicable to the clinical decision support process.

My role here today – as I understand it – is to explain from a regulatory perspective the use of big data and machine learning practices in financial markets. The purpose is to facilitate a conversation of how it might be relevant to the regulation of clinical decision support.

When AMIA approached me with the idea, I was immediately intrigued. For years I had looked at the medical sciences with envy. This is where you get to experiment with randomized control trials (RCTs) to understand the causal effects of treatments. This could be a powerful tool for understanding the efficacy of securities markets policy.[1] But RCT-like experiments have had only minimal uptake in financial market regulation. Public companies and other market participants have little incentive to be treated. It is not generally the case that death or despair is not on their doorstep. And if it is, they don't make good test subjects. Regulatory objectives are often intended to limit the practices of healthy firms – keep them from inappropriately benefiting at the expense of others. So, differential treatment is generally viewed as a recipe for competitive harm. Imagine telling Amazon, but not Apple, that they would be required to disclosure sensitive information, just to understand whether it was material to investors? It is a regulatory non-starter.

The prospect of speaking here opened a line of inquiry that I hadn't previously considered. Is there something that the medical sciences and informatics community could learn from financial markets? There might not be RCTs to draw from, but securities markets regulators have permitted the rapid adoption of machine learning methods in financial decision-making.

Admittedly, this is in large part due to absence of rules strictly forbidding it. But the SEC has generally taken a permissive, wait-and-see regulatory approach to innovation. This often occurs by granting exemptive relief from existing rules. The purpose to evaluate their continued relevance. This is the SEC's version of a regulatory sandbox, which facilitates a different type of learning experience.

Over the years there have been a lot of financial market lessons to learn from. Many innovations have not gone well. In fact, some have gone exceedingly bad. I suspect a few have already come to your mind. Among them are a class that I think are relevant to the discussion today – those that relinquish human control of decisions. Most notably, with algorithmic trading. But also, with asset pricing, portfolio allocation, liquidity risk management, and fraud detection. I'm going to cover a few examples today – showing both out right failure at one end of the spectrum, and underperformance and unrealized risks at the other.

What is machine learning?

An evolving concept that poses a challenge to regulators

Before I dive in, I think it makes sense to start with some level setting remarks about the definition of machine learning. I gave my first machine learning talk in 2015. At that time, Wikipedia defined the term as "the study of algorithms that could learn from data." By 2018 their posted definition was "a field in computer science that gives computers the ability to learn without being explicitly programmed." As of this week, Wikipedia says it is the "study of algorithms and statistical models that computer systems use to perform a specific task without using explicit instructions, relying on patterns and inference instead."

So, when we talk about regulating the use machine learning, we need to first recognize that it is a bit of an elusive concept. The semantics have changed over time, and I suspect they will continue to do so. This can be a challenge to a regulator seeking to draw bright lines around practices that use it.

Wikipedia's inclusion of statistical models in its most recent definition acknowledges what the social sciences have long recognized – the field of computer science is reinventing what, in many ways, already existed. Machine learning emerged from a body of techniques and methods first introduced by statisticians. Many sat dormant on the shelves of concept and theory until the necessary data and computing resources arrived to make them a reality. Computer scientists were first to recognize the new opportunities.

But as these definitions also imply, machine learning is more than just algorithms and models. It is as much about how they are applied. This is where computer scientists have excelled; they have proved better than social scientists at adapting the methods to real world problems.

One reason for the success of computer scientists is that they have unshackled themselves from the social science requirement of understanding why the models work. They are relatively unconcerned about the statistical significance of the model factors. They care more about the overall predictive power of a model.

To that end, they pursue associations, interactions, and non-linearities unencumbered by a strict need for human understanding. And the methods they use to get there are rather meta; they use algorithms to find the most relevant algorithms. If the objective is predictive power only, then it is easier for a machine to evaluate hundreds and thousands of model specifications to find the right one. Removing the human in model selection is a tangible example of machine learning.

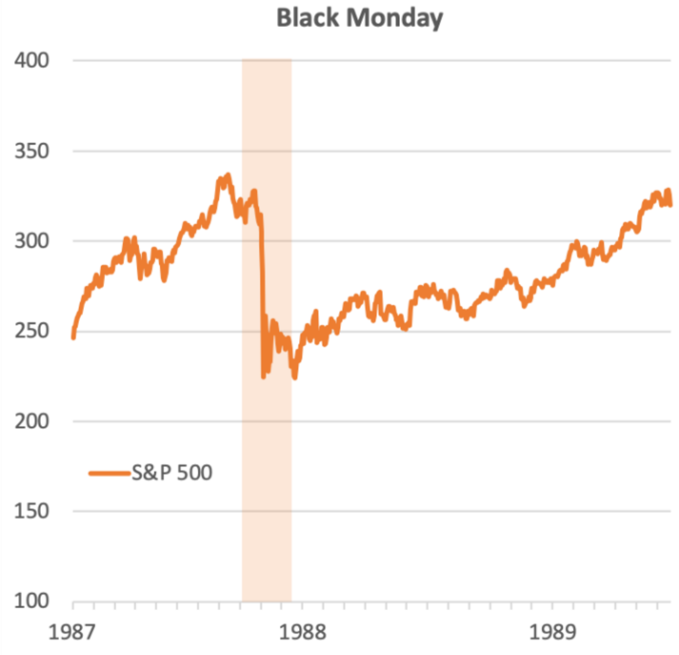
In financial markets, where algorithms have long had a place, these developments pose new risks. Removing human understanding and judgement in the application of models can be catastrophic when they go wrong. The predictive consequences from a bad retirement decision is far more severe than a bad consumer purchase recommendation or Alexa music play suggestion. There are no do-overs.

Moreover, algorithms in financial markets have already demonstrated great capacity for costly consequences. There is no doubt that they have on average improved our lives by increasing the efficiency of capital market operations. But their goofs have been on an order of magnitude that few humans could have achieved.

1987 Market Crash

Algorithmic risk first appears in financial markets

Regulators first thought about the need to evaluate the risks of algorithmic trading more than three decades ago. On Monday, October 19th – also known as Black Monday – the Dow Jones Industrial Average dropped 23%. It remains today the largest single day drop in the history of the index and caused widespread panic and disruption in the financial system.



Source data: Center for Research in Securities Prices

A presidential task force was commissioned to understand what happened. In 1988 they issued a report.[2] In it they cited a number of economic factors that contributed to the downward pressure on prices, but none were identified as the cause of the crash. Instead, the task force pointed to program trading, which acted as an accelerant of the price declines.

At that time, large institutions offered a product called 'portfolio insurance' to their clients.[3] The objective was to limit their losses in a declining market. They used computer algorithms to calculate how much insurance to buy, which was done by selling futures contracts. As futures prices fell, other large market participants used the NYSE's (Designated Order Turnaround or "DOT") automated execution system to engage in arbitrage between futures and equities markets. In this way, additional portfolio insurance purchases in futures markets drove equity prices down.

The basic effect of the computer algorithms was to sell stock as the prices fell, which mechanically induced the selling of more stock. This is believed to have exacerbated the price effects of fundamental information in the market. And it is some of the first evidence of rules-based, algorithmic trading that removes human judgement, induces investor herding, and makes markets fragile.[4]

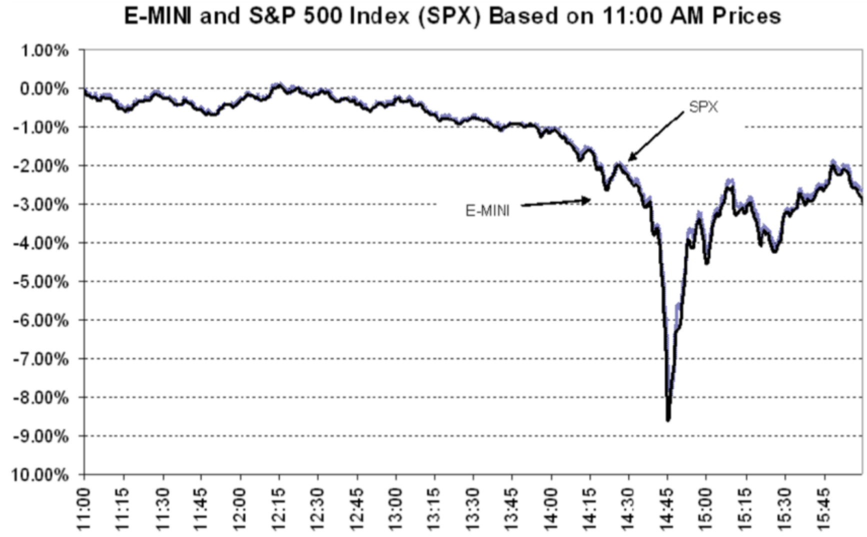
The problem, one that endures today, is that market participants often use models to make investment decisions that are locally optimal, for an individual investor or institution. They do not always account for broader environmental factors, including the impact of their collective actions. In economics, this can be explained as the difference between a partial and general equilibrium model. Partial equilibrium models are easier to design and implement, but they don't account for the potentially important feedbacks considered in a general equilibrium model.[5]

2010 Flash Crash

Algo trading temporarily moves market by $1 trillion

It is likely that the algorithms used at the time of the 1987 crash were simple regression models, a basic method in the modern machine learning toolbox. The response at that time was not to regulate their use. Instead, the task force recommended that "circuit breaker mechanisms (such as price limits and coordinated trading halts) should be formulated and implemented to protect the market system." Algorithmic trading would continue, but if models went awry, trading would pause before there was a crash. This would allow humans to take stock of the situation and rationally respond.

In the 1990's, new computerized trading systems called electronic communication networks (ECNs) emerged. Remember, Instanet, Island, and Archipelago? They allowed traders to bypass exchanges and match orders with each other at lower cost. This jumpstarted the online trading industry we know today. Regulators approved of the new competition and in 2006 adopted Regulation NMS (National Market System) to codify open access based on best price execution. This was the death knell for the NYSE floor traders. By 2008 they were being phased out in favor of fully electronic trading.



On May 6, 2010, the market experienced its first flash crash. According to a SEC-CFTC report, an automated execution algorithm initiated $4 billion sell order in futures market without regard to price or time.[6] Like with the 1987 Crash, cross market hedging created severe downward price pressure on equity markets. The market dropped nearly 10% in the span of a few minutes.

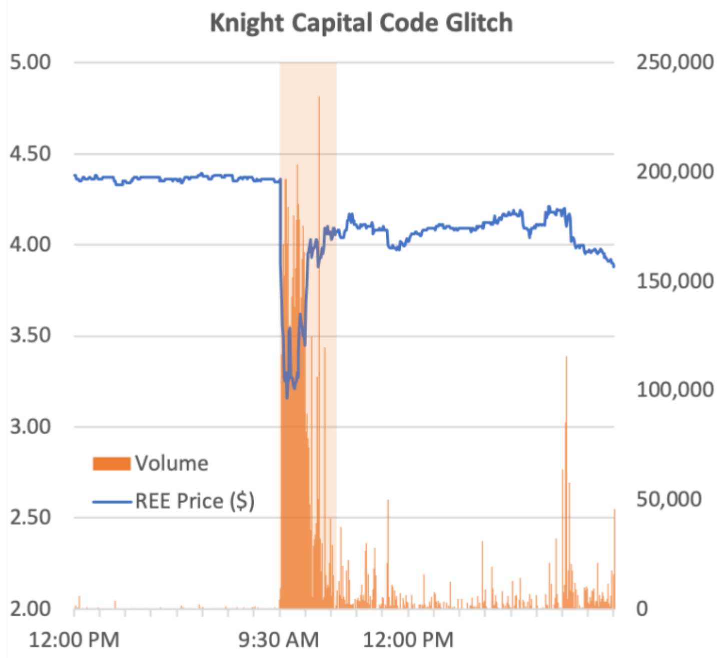
By this time, high frequency traders (HFTs) accounted for 80% of the dollar volume of US equity trades.[7] The models underlying the trading were proprietary and ill-understood by regulators. The speed with which the crash occurred and then recovered was stunning. It was over before humans could process what was happening. And the market-wide breakers adopted after Black Monday were never tripped.

Once again, an algorithm had caused serious disruption. One trillion dollars in market capitalization temporarily vanished because of a $4 billion automated trade. It led to further tightening of the price bands and conditions for trading halts, but no regulation was introduced to limit the use of algorithms.[8] The regulatory approach continued to favor reaction over prevention. Algorithmic innovation in trading continued under a stricter monitoring regime.

2012 Knight Capital Trading Glitch

A $460 million coding error

This regulatory approach came into question on August 1st, 2012. That morning, Knight Capital, an equity market maker, erroneously sent more than 4 million orders into the market when attempting to fill just 212 customer orders. In just 45 minutes, Knight had assumed a net long position in 80 stocks of approximately $3.5 billion and net short position in 74 stocks of approximately $3.15 billion.[9] Unwinding the unwanted positions resulted in a loss to the Knight Capital of $460 million.



Rare Element Resources intraday price and volume from WRDS TAQ

Many of the stocks Knight erroneously traded reached volumes far greater than their typically daily average. And like the 2010 flash crash, prices temporarily moved away from their fundamental values. Radio Shack shares increased 27% in the first few minutes of trading before falling back to the previous day’s close. Rare Element Resources, which Knight shorted, fell 29% on more than 3 billion shares traded. The day before, volume was less than a million shares.

Then Chairman of the SEC, Mary Schapiro, called it an unacceptable event.[10] Knight was fined $12 million for not having controls designed to limit the risks associated with their direct access to the markets. The firm survived the incident with a cash infusion from private investors and was subsequently acquired by another securities firm.

Unfortunately for Knight, rules tightening the price bands and conditions for trading halts following the 2010 flash crash were not yet effective. Exchanges were still in the process of implementing a limit up-limit down mechanism that would have paused trading if prices moved too fast. This could have prevented some of the disruption and ultimate trading losses.

The impact of this event led to the 2014 adoption of Regulation SCI.[11] The acronym stands for Systems Compliance and Integrity. Its aim was to restore investor confidence in markets by regulating the technology controls at the largest market participants – those most essential to the efficient functioning of the U.S. securities markets. The measures, like with past SEC actions, did not limit the use of algorithms. It focused on the policies and procedures at entities using them. It also gave regulators expanded tools to discipline disruptive behavior.

This episode was another demonstration that computer algorithms can create havoc in ways it is hard to imagine a human could attain. In the old days, losing half a billion dollars took months and years of poor decision making or skullduggery. Now it takes less than an hour.

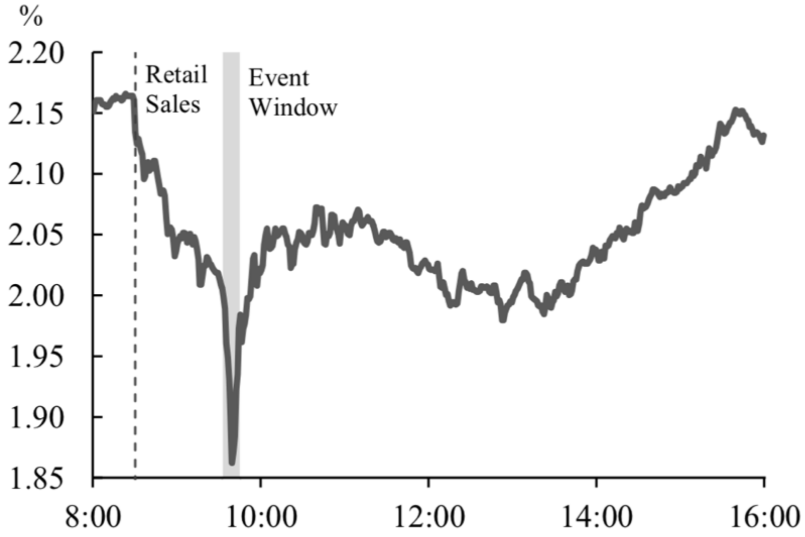
2014 Treasury Market Flash Rally

A market disruption with still unknown cause

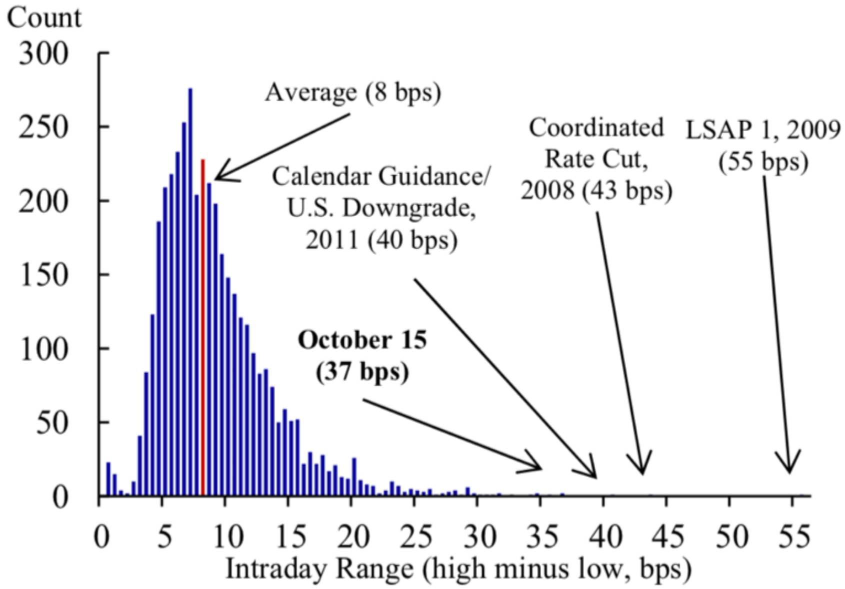
In 2014, when the term machine learning began entering the vocabulary of financial market participants, a new type of flash crash emerged. On October 15 of that year, treasury yields experienced unusually high and unexplained volatility. The 37-basis-point trading range over the day was historic in size.

During one ten-minute span, the ten-year yield dropped and rapidly rebounded 16 basis points. It was dubbed a flash rally because treasury prices are inversely related to yields.

Only the US debt downgrade in 2011 and two financial crisis events – the coordinated rate cut in 2008 and announcement of large scale asset purchases in 2009 – proved more volatile. Yet, the only notable news on October 15 was the release of somewhat weaker-than-expected U.S. retail sales.



Joint staff report on the U.S. Treasury Market on October 15, 2014



Joint staff report on the U.S. Treasury Market on October 15, 2014

To this day, the brightest minds in the regulatory world can't explain why it happened. After a yearlong investigation, an official report by staffs of the U.S. Treasury, Board of Governors, New York Fed, CFTC, and SEC offered only vague ideas. [12] An early finger was pointed at principal trading firms (PTFs), the algorithmic frequency traders in treasury markets. But the government report did not uncover any smoking gun evidence. They could not isolate any aberrant trading from a coding error like with Knight Capital. And they did not find a patient zero trade like what triggered the 2010 flash crash.

That the joint regulatory effort could not explain what happened is scary. The large team had access to the fully history of trading records, the market participants doing the trading, and world class analytical tools.

But they did provide an interesting observation. The most volatile period of the day was dominated by multiple PTFs trading with each other using different strategies. During this period, bank-dealers widened their spreads, meaning the human conduits for real supply and demand in the market stepped away from trading. This left the PTF algorithms to trade with each other. Some were aggressive – trading in the direction of price movement. Some were passive – leaning against the trading wind.

The report did not offer an interpretation for how this contributed to the volatility. But it doesn't take much imagination to hypothesize a bot war. Algorithms are trained to act on signals. In this case, estimating the inventory needs of bank-dealers and their customers. When the bank-dealers stepped away, the algorithms lost their primary signals. What then, informed their trading? The trading decisions of other uninformed algorithms?

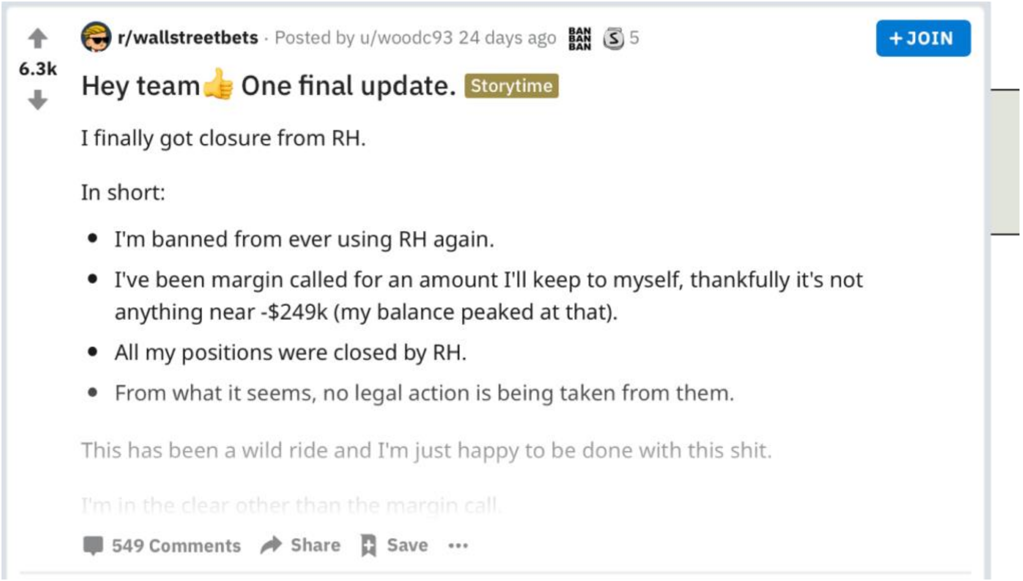
User abuse of algorithms

The infinite money cheat code

The most recent example of a software glitch in equity trading is on a far smaller scale than the previous examples. And it doesn't involve algorithmic trading. But it demonstrates an important risk for all software developers. If there is a way for a user to abuse or misuse an application, they will find it.

A month ago today, a vulnerability at the no-fee online trading firm Robinhood was reported by several news outlets.[13] Users of the platform were purportedly allowed to borrow money against their holdings in excess of the legally permissible 50%. A glitch in the code treated certain securities purchased as additional collateral to borrow against. This flaw was shared in a Reddit user group. It allowed retail investors to lever up the same way Bear Sterns did leading into the financial crisis. And the self-reported results weren't much different.

One Reddit user claimed to borrow $1.3 million on a $15,000 deposit. He reported losing $180,000 trading AMD put options – another form of (notional) leverage.[14] The days following the code bug saw more users reporting the use of even greater leverage with similarly bad outcomes. The experiences are reminiscent of the hubris that infected the dot.com era. A good illustration that some behaviors don't change; they just move across generations.



r/wallstreetbets · Posted by u/woodc93 24 days ago

Hey team👍 One final update.

I finally got closure from RH.

In short:

- I'm banned from ever using RH again.
- I've been margin called for an amount I'll keep to myself, thankfully it's not anything near -$249k (my balance peaked at that).
- All my positions were closed by RH.
- From what it seems, no legal action is being taken from them.

This has been a wild ride and I'm just happy to be done with this shit.

I'm in the clear other than the margin call.

These 'clever' investors learned that leverage makes the good times better and the bad times worse. A Robinhood spokesperson confirmed with Bloomberg that they identified a small number of accounts engaging in problematic trading and made a permanent update to their systems to prevent further abuse. One Reddit user put it more succinctly: "banned from ever using Robinhood again."

It is too soon to know what the regulatory response will be. The focus has thus far been on the colorful user experiences. And some will cite caveat emptor – these investors learned a valuable lesson. But a violation of Regulation T, which limits the use of leverage in margin trading, is a significant allegation for Robinhood.[15] The regulation protects retail investors who may not fully appreciate the larger scale risk of leverage. It also protects the financial system from the potentially destructive effect of its collective use by the market.

The example also highlights the risk of FinTech more broadly. From the west coast, you sometimes hear it branded TechFin, reflecting a desire to put 'technology' in front of the old school practices of 'finance'. But as I alluded to before, disruption in financial services can have more lasting consequences than common product market decisions. Getting someone's movie recommendation wrong does less harm than a bad investment outcome. Regulators may decide to make this a reinforcing example of why the existing rules are there.

Regulation of machine learning

Should the focus be on the algorithms or the entities using them?

At this point you may be wondering about the role of machine learning in these examples. I think it is safe to assume that if any of the algorithms prior to 2015 were using machine learning methods, the users didn't know it. Computer science was just beginning to claim finance as part of their domain. I think it is equally safe to assume that machine learning methods are imbedded in most of the algorithms in use today. But the strict answer is that we don't know. Because regulators do not currently restrict or approve the use of algorithms in financial trading, products, and services, there is only anecdotal evidence to rely on.

That machine learning is nonetheless embedded in current financial market practices is reinforced by regulators acknowledging that they use it too. That's right, regulators commonly use machine learning methods in their supervisory activities. And they have been for a while.[16] Natural language processing techniques helps them analyze narrative disclosure in regulatory filings. Unsupervised learning methods identify latent topics – that is, patterns in regulatory disclosures that humans are unlikely to detect. These use random forest models to connect these topics to historical inspections and enforcement actions to predict the likelihood of future transgressions. And if you are thinking about insider trading, this is where the most sophisticated methods reside.[17] If you do it, regulators will likely know about it.

For a regulator, experience using machine learning methods provides valuable context on how to regulate them. Most notably, it brings acute awareness to the performance sensitivity an algorithm has to its applied environment. Recent experiences in financial markets shows how hard it is to predict how they will operate and interact in a complex system, particularly when inputs to the models are constantly changing and outside the control of the modeler. Case in point: five federal regulators took a year to conclude that they didn't understand what caused the treasury market flash rally.

Short of a draconian ban on their use, machine learning methods in financial markets will continue to generate the occasional bad outcome. Regulators do not have qualified staff in requisite numbers to systematically review and approve models. Even if they did, it is impossible to conceive every scenario that the real world has to offer. Backtesting a model is only as good as the training data you give it. In financial markets, the future rarely looks like the past, and there is no substitute for going live.

The SEC's general approach of entity-based regulation is a more practical course than it is ideological. Putting the responsibility of technology controls on the innovator is more efficient than introducing an algorithmic approval process. Putting market protections in place to limit potential damage from errant algorithms is easier than preventing it. With algorithmic trading, this means pecuniary penalties for disruptive behavior, and when it occurs, slowing time with pauses and halts to let human decision-making rejoin the price discovery process.

Outsourcing the supervision critical market functions in this way has engendered costly learning experiences in financial markets, just as it has in other areas of regulation (e.g., Boeing 737 Max).

That the Food and Drug Administration opened a public comment for a proposed regulatory framework on the use of machine learning and artificial intelligence in software as a medical device provides a new set of challenges and tradeoffs to the risks and rewards of technology. [18] And the use of machine learning technology in clinical support faces many of the same challenges it faces in financial market applications. Most notably, there is an inherent human distrust in a blackbox decisions and recommendations. Humans want interpretability. Social scientists have understood this for generations. Knowing the reason for a outcome can be more important than the predicting it.

I hope that the reactor panel to remarks can make sense of my regulatory experience in the context of clinical support. And I look forward to hearing where there are commonalities and differences between finance and medicine.

To close, I would like to offer one last thought on the use of randomized control trials. It is ironic that financial regulators are reticent to apply similar methods in determining policy, particularly when considering the magnitude of disruption and harm that technological innovation has repeatedly engendered in markets. I would find it instructive, and a lesson to financial market regulators, if the medical sciences ultimately used RTCs to assess the efficacy of AI/ML technology.

It has been my pleasure to speak here today.

Some of the concluding remarks may not accurately reflect the delivered address as they were not formalized in writing at that time.

[1] See, e.g., Leuz, Christian, Evidence-Based Policymaking: Promise, Challenges and Opportunities for Accounting and Financial Markets Research (April 12, 2018). https://ssrn.com/abstract=3161401

[2] The Report of the Presidential Task Force on Market mechanisms (a.k.a. The Brady Report), 1988, found at https://www.armstrongeconomics.com/wp-content/uploads/2014/01/BRADY-REPORT-Full-text-of-_Report-of-the-Presidential-Task-Force-on-Market-Mechanisms.pdf

[3] Securities and Exchange Commission Report, 1988, The October 1987 Market Break. *See also* Carlson, Mark A., A Brief History of the 1987 Stock Market Crash With a Discussion of the Federal Reserve Response (April 2007). FEDS Working Paper No. 2007-13. https://ssrn.com/abstract=982615

[4] Bauguess, Scott W., Market Fragility and Interconnectedness in the Asset Management Industry (June 20, 2017). SEC Keynote Address: Buy-Side Risk USA Conference 2017. Available at SSRN: https://ssrn.com/abstract=3226541

[5] See, e.g., https://en.wikipedia.org/wiki/Partial_equilibrium

[6] Findings Regarding the Market Events of May 6, 2010: Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues. https://www.sec.gov/news/studies/2010/marketevents-report.pdf

[7] Zhang, Frank, High-Frequency Trading, Stock Volatility, and Price Discovery (December 2010). Available at SSRN: https://ssrn.com/abstract=1691679

[8] The anti-disruptive trading measure known as the limit up-limit down mechanism was approved June 1, 2012. See, https://www.sec.gov/news/press-release/2012-2012-107htm

[9] For a more detailed explanation, see https://www.sec.gov/litigation/admin/2013/34-70694.pdf . See also, Kirilenko, Andrei A. and Lo, Andrew W., Moore's Law vs. Murphy's Law: Algorithmic Trading and Its Discontents (March 19, 2013). Journal of Economic Perspectives (2013). https://ssrn.com/abstract=2235963

[10] Chairman Schapiro Statement on Knight Capital Group Trading Issue: https://www.sec.gov/news/press-release/2012-2012-151htm

[11] Open meeting statement by SEC Chair Mary Jo White on the adoption of Regulation SCI: https://www.sec.gov/news/public-statement/spch112014mjw

[12] Joint staff report on the U.S. Treasury Market on October 15, 2014, written by the U.S. Department of the Treasury, Board of Governors of the Federal Reserve System, Federal Reserve Bank of New York, U.S. Securities and Exchange Commission, and U.S. Commodity Futures Trading Commission

https://home.treasury.gov/system/files/276/joint-staff-report-the-us-treasury-market-on-10-15-2014.pdf

[13] Brandon Kochkodin, "Robinhood traders discovered a glitch that gave them 'infinite leverage'," Bloomberg, Nov 5, 2019. https://www.bloomberg.com/news/articles/2019-11-05/robinhood-has-a-glitch-that-gives-traders-infinite-leverage

[14] See self-reported abuse: Ben Winck, "A stock-trading Reddit forum has minted a group of hall-of-famers who best exploited Robinhood's 'infinite leverage' glitch. Here's how much money each has amassed through the hack." MarketsInsider, Nov 11, 2019. https://markets.businessinsider.com/news/stocks/robinhood-infinite-leverage-free-money-hall-of-fame-position-amounts-2019-11-1028670517#moonyachts3

[15] FINRA overview of margin requirements: "In general, under Federal Reserve Board Regulation T, firms can lend a customer up to 50 percent of the total purchase price of a margin security for new, or initial, purchases." See, https://www.finra.org/rules-guidance/key-topics/margin-accounts

[16] Bauguess, Scott W., The Role of Big Data, Machine Learning, and AI in Assessing Risks: A Regulatory Perspective (June 21, 2017). SEC Keynote Address: OpRisk North America 2017. Available at SSRN: https://ssrn.com/abstract=3226514

[17] The SEC leadership has periodically discussed its insider trading detection algorithms that go by the acronyms of ARTEMIS and ATLAS. See, e.g., https://www.sec.gov/news/statement/statement-mjw-040816.html; https://www.sec.gov/news/speech/piwowar-old-fields-new-corn-innovation-technology-law; and https://www.sec.gov/news/speech/clayton-keynote-mid-atlantic-regional-conference-2019

[18] Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (AsMD), https://www.fda.gov/media/122535/download