September 25, 2012

Securities and Exchange Commission
100 F St. NW
Washington, DC

In re: Technology and Trading Roundtable, File Number 4-652.

Thank you for the chance to comment for the Technology and Trading Roundtable ("Roundtable"). The Roundtable is a welcome start to what should be decisive action by the SEC in the face of repeated technology catastrophes this year. According to an August 2012 Tabb Group survey, half of buy-side survey respondents had weak or very weak confidence in today's markets, and two-thirds want regulators to act very fast or extremely fast to protect markets from flawed technology, as do almost 60% of sell-side respondents. While technology problems aren't new, the current rate of catastrophic error is something we haven't seen before. It shows how easily markets are disrupted when even just a few people, a few people with enormous power because of the technology at their fingertips, make a mistake. We're left to wonder whether the U.S. stock market is at the mercy of, as Tom Joyce of Knight Capital remarkably said of some of his own employees, a series of knuckleheads.

Technology error rates are in no small part a function of the rate of change, and change happens on millisecond and even microsecond timescales in today's markets. In recent technology errors involving BATS, Direct Edge, Infinium, Knight, Nasdaq, and NYSE, nothing so captures the times as Nasdaq's Facebook misadventure. Its error, as Nasdaq has described it, literally came down to timing by the millisecond.

To explore that kind of risk, the Federal Reserve Bank of Chicago recently published results from a series of in-depth risk management interviews it conducted with more than 30 firms inside the world of high-speed trading, from exchanges to clearing firms. Most important for the Roundtable's discussions, the Fed interviewed nine different proprietary trading firms for the survey. The Fed's results (see http://www.chicagofed.org/digital_assets/publications/policy_discussion_papers/2012/PDP2012-1.pdf) include the most detailed and insightful examination of risk management practices at these firms ever published.

The document is an 18-page roadmap of the best and worst practices in high-speed proprietary trading. What's most revealing is that risk management is left almost entirely up to the trading firms themselves to decide, with highly varying practices and highly varying results. Though some clearing firms regularly audit the trading firms' overall risk management practices, for the most part these firms have only their own self-interest to guide them. Regulators aren't mentioned, except to hope they stay away.

In one light, all this is a good example of how self-interest incents risk management. Essentially unsupervised firms seem to manage risk well because it's in their self-interest to do it. But we have too many examples now of firms that overlooked their longer term interests, or deluded themselves into believing they had their risks under control, and people made mistakes; we all hope to act in our own best self-interest, but we also misjudge risk and consistently overestimate our own talents. Amplified by technology, those misjudgments have systemic implications. Markets work. But markets also break in ways and on a scale they never did before, with social and economic costs borne by everyone. The Flash

Crash, Infinium, BATS, Nasdaq, Knight - and more - prove that as well as it can be proved. "It is clear that at the pace we all operate, I was mistaken," Reuters quoted Tom Joyce as saying, "regulatory risk was not our biggest issue, operational risk was and we unfortunately proved it."

It's our risk too because technology has changed markets the way gunpowder changed the velocity of lead. Speed is a qualitative change. When it is unremarkable for firms to submit 10,000 orders a second, the possibility of a mishap is exponentially greater than it was just 10 years ago, when 100 orders a second was a breathtaking pace. Consistently misjudging where and how risk is at work, the industry today seems determined to shoot itself in the foot over and over again, stopping only to reload.

"No. Why?"

Error prevention starts with best business practices in technology design, development, testing, and implementation. Best practices include business and functional requirements definitions reviewed by compliance and risk management, disciplined engineering that incorporates robust real-time error detection and correction, comprehensive and reproducible quality assurance testing by an independent quality assurance function, and staged systems integration and implementation in a tightly controlled production environment.

The firms the Fed interviewed were happy with how they managed risk and prevented errors. The Fed summarized what firms said about risk management by writing "Relying on existing industry best practice documents for risk management is desirable. Regulatory guidance on risk management is not needed because trading firms have a better understanding of risks than regulators." In other words, the industry wants to be left alone because the industry thinks it knows what it's doing.

That's not what the Fed found, at least not everywhere. The Fed explored technology practices and found that "Depending on the trading firm, the life cycle for the development, testing, and deployment of a new trading strategy ranges from minutes to months to one year. At a few firms, new trading strategies are quickly implemented by tweaking code from existing strategies and placing new code into production in a matter of minutes." When a firm tweaks code and puts it into production in a matter of minutes, it's the information technology equivalent of a surgeon who shotguns a beer, picks his nose, and walks into an operating room. Recently, Traders Magazine reported that technology executives told it "software development processes and procedures are often haphazard. Pressure to rush a new feature to market can override the need to get it right, they say."

Unsurprisingly, the Fed found one firm that "had two incidents of [an] out of control algorithm. To address the first incident, the firm added fat finger and credit checks to its pre trade risk controls. The second out of control algorithm was caused by a software bug that was introduced when fixing the error code that caused the first incident." The Fed noted that "Six of the nine firms interviewed had such occurrences or got caught up in other firms' out of control algorithms." Mysteriously, "Error in one firms' automated system impacted prices, but the firm declined to provide specific details related to what went wrong."

Error prevention also includes real-time controls on software. How do firms manage the risk of an algorithm going berserk? Every firm told the Fed their controls include pre-trade checks on order sizes and position limits; almost all firms had credit limits and P&L limits; most firms had controls on order rates; only half the firms had controls on order prices. Tellingly, however, the Fed said that "Most firms apply fewer pre-trade risk checks to some strategies to reduce latency (delays)"; where and how

they skimp wasn't noted. Though every firm said it had a kill switch, most kill switches are manual and so operate at (complex) human cognition and reaction times of at best two seconds, according to research in decision theory, enough time for any firm to spray the markets with tens or even hundreds of thousands of orders. In the real world, where risk operates in microseconds, manual intervention will never be quick enough. The Financial Times wrote that it took Infinium not two but 24 seconds to kill an out-of-control algorithm. Depending on the account, it took as many as 45 minutes to interrupt Knight's out-of-control software.

Tom Joyce appeared on Bloomberg on September 21 and was asked what changes, if any, his new owners were going to make at Knight Capital in light of its disaster. "None," he replied. Stephanie Ruhle of Bloomberg then asked, "After all that happened they're not looking to change anything in the firm?" Joyce answered, "No. Why?" Perhaps because, someone might note, his firm lost an average $10 million a minute while it distorted prices and caused chaos, or perhaps because his firm almost bled out before the hemorrhage could be tied off. (Joyce suggested that maybe - maybe -volume-based circuit breakers might help, presumably because he imagines they could have saved Knight. Volume-based circuit breakers are an interesting thought experiment. Exchange circuit breakers that go off when volumes spike but prices don't will halt stocks that are, well, *liquid*.)

A parade of knuckleheads

After all this mess, and after all this hubris, it's obvious the industry doesn't always know what it's doing, and it shouldn't be left alone to follow its own guidelines, however good they look on paper. We don't know specifically what sequences of events created problems at BATS, Direct Edge, Infinium, Knight, Nasdaq, and NYSE, but one or more of human error, business practices, competitive pressures, and risk operating at speeds beyond comprehension certainly played a part in some or all of them. Regulators can't prevent all human error, and regulators should encourage competition, but regulators can certainly address any business practices that increase the probability of human error, and regulators can slow risk down.

As markets became highly automated and floor-based trading disappeared, markets lost critical abilities to police errors and runaway trading even as errors and runaways started to erupt in milliseconds. With this year already full of calamities and every reason to believe next year will bring more of the same, the SEC should pass rules requiring that market centers and firms with direct access to them raise their game.

The SEC's Automation Review Policy ("ARP") is a useful example. While it is nominally a "voluntary" policy, for stock and options exchanges ARP is mandatory in fact if not in law. Decades of ARP reviews haven't cured all that ails exchange technology, but at least the exchanges now reliably keep the lights on, something that was by no means guaranteed before ARP. That the exchanges kept trading in the autumn of 2008 despite record volume and volatility was no testament at all to our deregulated free-for-all markets, but it certainly was a compelling testament to 20 years of ARP.

SEC officials have suggested in public that ARP could become mandatory and that "large" firms could be covered by the policy. Assuming it would include at least all the ATSes and the larger market makers, that's a good beginning, but the SEC should go further. While the SEC might not have the resources to include every firm with direct market access in its ARP reviews, every firm with direct market access, as well as the exchanges, can earn ISO 9000 quality management certification. Technology is the physical embodiment of compliance and regulation, and quality assurance is the only proof we'll ever

have the embodiment is correct. (Have any of the firms in the headlines this year cut, outsourced, reengineered, "right-sized," or off-shored or near-shored quality assurance, or otherwise recently lowered quality assurance budgets?) While the ISO 9000 standard is vague and can be gamed - the same can be said for ARP - certification will at least bring some kind of baseline standard to the industry and put a floor on development and quality assurance business practices. As the Fed found, today these practices can vary from strong controls to very few controls at all.

ARP and ISO 9000 are only a start. Regulators must also insist that firms have appropriate, to borrow from Nasdaq's March 2012 settlement with Getco, "supervisory and operational risk controls for the oversight and operation of algorithms" and "procedures and controls related to the creation, modification, usage, and testing of trading algorithms, and to the review and oversight of levels of message traffic and wash sales and other potentially improper trading activity." In particular, FINRA should enforce baseline technology and risk controls at every relevant firm under its umbrella. The Fed's recommendations are a good start.

Regulator supervision should be backed up by a strict liability standard for disruptive technology. Almost every day the market data firm Nanex highlights obvious incidents of algorithms spinning out of control. For example, what legitimate purpose could there be for a low-volume stock to explode with tens of thousands of quotes - or more - in a few seconds, on no news and with no trades? These are obvious cases where the market has lost its mind. Regulators should go after them quickly and severely. They are disruptive whether they are deliberate or not. The only effective response to these events is tough enforcement.

Finally, risk must slow down. Regulators should mandate 50 or 100 millisecond order lifetime minimums. Speed limits might at least have saved Nasdaq - and the rest of us - from its disaster. High frequency firms will complain they'll get picked off, that spreads will get bigger and markets will suffer, but remember that a decade ago, with the technology of the day, these firms somehow managed to thrive with 50 millisecond latency and spreads fell dramatically. From the beginning of decimalization to the end of 2002, spreads dropped by about 15 cents, or 75%. From the end of 2002 to today, as latency dropped from 50 milliseconds to 100 microseconds - 500 times faster - spreads haven't changed much at all in absolute terms. In other words, with a penny tick size and 50 millisecond latency we got almost all the market quality gains we're going to get from speed. Speed limits will also allow regulators to insist on, and firms to implement, robust risk controls. What we have instead is a risk management race to zero, as we stagger from one catastrophe to another behind a parade of knuckleheads.

Sincerely,

R. T. Leuchtkafer