University of Pittsburgh
School of Law
Hickton Center for Community Legal Services and Clinical Legal Education

Barco Law Building
3900 Forbes Avenue
Suite 420
Pittsburgh, PA 15260
(P) 412-648-1300
(F) 412-648-1947

Mailing Address
P.O. Box 7226
Pittsburgh, PA 15213

March 8, 2024

**Via email**
pubcom@finra.org
Jennifer Piorko Mitchell
Office of the Corporate Secretary
FINRA
1735 K Street, NW
Washington, DC 20006-1506

**RE: University of Pittsburgh Securities Arbitration Clinic's response to the "Quantum Computing and the Implications for the Securities Industry" request for comment.**

**By:** Professor Alice L. Stewart,* Professor Rachael Shaw,* Kyle J. Bobeck,* Danny O'Byrne,* Wesley Li,* & Justin Lindsay.*

**Contents:**



* Director of Legal Clinics and Associate Professor of Law, Director of the University of Pittsburgh Securities Arbitration Clinic
* Adjunct Professor of Law.
* J.D. Candidate, University of Pittsburgh School of Law, Class of 2024.
* J.D. Candidate, University of Pittsburgh School of Law, Class of 2025.
* J.D. Candidate, University of Pittsburgh School of Law, Class of 2024.
* J.D. Candidate, University of Pittsburgh School of Law, Class of 2024.

## I. Introduction

The University of Pittsburgh operates several legal clinics to aid persons of lower income and increase access to justice.[1] The Securities Arbitration Clinic does so by representing small investors in disputes through arbitration before the Financial Industry Regulatory Authority (FINRA).[2] In addition, the clinic has filed as amicus curiae on securities issues before the courts, the students also research and comment on current securities issues.

The University of Pittsburgh Securities Arbitration Clinic represents aggrieved investors with disputes under $75,000—disputes that are often deemed "too small" to warrant representation on a contingent fee basis and traditional legal clinics are not prepared to handle. The clients of the clinic are often elderly, economically disadvantaged, and unsophisticated investors that are frequently taken advantage of by scammers and unscrupulous brokers. Our role is to investigate their claims, advocate in arbitration, and proactively advocate for them by addressing issues that future clients may not be aware of by writing comments such as this. To that end, the University of Pittsburgh Securities Arbitration Clinic submits the following in response to FINRA's request for comments on its publication "Quantum Computing and the Implications for the Securities Industry."[3]

## II. Quantum Computing

Quantum computing, based on quantum bits, can handle complex calculations faster and more efficiently than classical computing, which relies on binary bits. This quantum advantage offers significant potential in finance for optimizing portfolios, speeding up financial modeling,

---

[1] *Clinics*, UNIV. OF PITT. SCH. OF L., https://www.law.pitt.edu/academics/experiential-learning-opportunities/clinics (last visited Feb. 29, 2024).
[2] *Securities Arbitration Clinic*, UNIV. OF PITT. SCH. OF L., https://www.law.pitt.edu/academics/experiential-learning-opportunities/clinics/securities-arbitration-clinic (last visited Feb. 29, 2024).
[3] *Quantum Computing and the Implications for the Securities Industry*, FINRA (Oct. 30, 2023), https://www.finra.org/rules-guidance/key-topics/fintech/report/quantum-computing [hereinafter "Request for Comment"].

and enhancing encryption. While classical computing has been the backbone of financial computations, quantum computing introduces a paradigm shift with its ability to process vast datasets simultaneously and solve problems previously deemed intractable, signaling a transformative impact on computational speed and problem-solving capabilities in the sector.

## III. The Case for FINRA Regulation

Quantum computing has the potential "to solve problems too large or complex for traditional computers."[4] As FINRA notes, "numerous financial institutions have begun experimenting with this evolving technology, given its potential to dramatically alter the types, and speed, of computations that are possible."[5] A Bank of America strategist recently said that the advent of quantum computing would be as revolutionary in the 2020s as smartphones were in the decade before.[6]

While it remains to be seen whether quantum computing has as large an effect as the quoted Bank of America analyst predicts, there's no doubt quantum computing—combined with other technological advances and computer functions such as blockchain, artificial intelligence, and robotics—will make its mark on the securities industry. FINRA has found that "major financial institutions have committed significant resources to the technology[,]" and some are "actively working with major cloud service providers to most efficiently access quantum computers."[7] In 2022, President Biden signed the Quantum Computing Cybersecurity Preparedness Act, a recognition of quantum computing's potential—and an attempt to get ahead of its potential harmful effects.[8]

---

[4] *Id.*
[5] *Id.*
[6] *Quantum Computing Will Be the Smartphone of the 2020s, Says Bank of America Strategist*, MARKETWATCH, (Dec. 12, 2019), https://www.marketwatch.com/story/quantum-computing-will-be-the-smartphone-of-the-2020s-says-bank-of-america-strategist-2019-12-12.
[7] Request for Comment, *supra*, note 3.
[8] H.R. 7535, 117th Cong. (as signed into law, Dec. 21, 2022).

FINRA details the potential uses and harmful effects of the forthcoming expansion of quantum commuting use in the securities industry. FINRA researchers sought input from "financial institutions, quantum computing hardware and software providers, academics, industry observers, government entities, security specialists and trade institutions."[9] The result is a paper focused on the impact of quantum computing on *large financial institutions*. The identified potential uses for quantum computing in the securities industry—optimization of trade execution, trade settlement, and investment portfolio design, as well as the ability to run more in-depth risk-assessment simulations—will be available only to the institutions that can afford the hefty price tag quantum computing will require, at least for the foreseeable future. FINRA also details the potential risks quantum computing brings, largely in the data security area.

**A. High(er) Frequency Trading**

As discussed in the introduction of this comment, the types of clients served in the Securities Arbitration Clinic are small investors who are unlikely to have access to quantum computing to optimize their trade settlements or run in-depth risk-assessment simulations. Large firms already employ high frequency trading platforms, using powerful computers to complete large orders in the blink of an eye. These complex algorithms allow large firms to make small profits on each transaction, which generates a significant return in the aggregate due to the sheer volume of trade their "supercomputers" can execute.[10]

Already, today's supercomputers can execute millions of transactions in seconds.[11] High-speed traders account for "over half of all daily stock trading."[12] And this is *before* the power of

[9] Request for Comment, *supra*, note 3.
[10] *High-Frequency Algorithmic Trading*, CHARLES SCHWAB (Jan. 23, 2023), https://www.schwab.com/learn/story/high-frequency-algorithmic-trading.
[11] *Id.*
[12] Ted Knutson, *HFT Mixed Bag for Retail Investors Say Experts*, FORBES (Sept. 24, 2018), https://www.forbes.com/sites/tedknutson/2018/09/24/retail-investors-helpedhurt-by-high-frequency-traders-experts-say/?sh=1b4b06925e5b.

quantum computing has been added to the mix. Small investors like those the Pitt Law Securities Arbitration Clinic represent cannot discern stock trends as quickly as high-frequency traders with complex algorithms and computers operating in terms of nanoseconds.[13] The introduction of quantum computing will only expand the discrepancy.

### B. Protection of Customer Data

FINRA notes in its paper that quantum computing offers potential threats to cybersecurity. Quantum computing could reduce—perhaps significantly—the time it takes to break the encryption that protects digitally stored information. Relevant to our clients, that information includes customers' personally identifiable information and trade orders placed on mobile applications. Large firms are best positioned to anticipate and prepare for attacks on their stored data, and FINRA is right to consider what standards it should require of firms.

### C. Conclusion

As FINRA considers offering guidance or modifications to its rules as it addresses the adoption of quantum computing, we urge the agency to take smaller investors like our clients into account when doing so. We urge FINRA to consider fairness in the high-frequency trading realm and to put the onus on firms to ensure client data is protected from quantum computing-enhanced encryption cracking attempts.

## IV. Data Safety Subject Areas for FINRA Regulation

While quantum computing has the potential "to solve problems too large or complex for traditional computers," it also can create problems, as traditional encryption keys and other data security practices face obsolescence.[14] Therefore, because analysts and national security officials

[13] Larry Harris, *What To Do About High-Frequency Trading*, CFA INSTITUTE (April 24, 2013), https://blogs.cfainstitute.org/investor/2013/04/24/what-to-do-about-high-frequency-trading/.
[14] Request for Comment, *supra* note 3.

fear hackers are stealing consumer data now to use when quantum computing technology becomes readily available, there is still time to prevent hackers from disrupting the securities industry.[15]

### A. Data Security

The importance of securing quantum computing data is exemplified by a problem that cost U.S. citizens 2.39 billion dollars in 2021—password compromise.[16] Currently, quantum computers are still in their infancy, and experts say it could still be a decade or more before quantum computers can accomplish anything worthwhile.[17] However, hackers—and likely "[a]dversaries and nation-states"—are using a "harvest now and decrypt later" strategy to pounce on consumer investors' passwords in the future.[18] Their goal is simple: they now collect sensitive, encrypted data in the hope that advances in quantum computing technology will allow them to bypass online banking passwords or two-factor authentication and zero out their victim's accounts.[19] Given that our clientele comprises elderly and unsophisticated investors, they are especially susceptible to practices like this and may lack the resources or knowledge needed to adequately secure their accounts against password compromise.

---

[15] Patrick Howell O'Neill, *The US is Worried that Hackers are Stealing Data Today so Quantum Computers can Crack it in a Decade*, MIT TECH. REV. (Nov. 3, 2021), https://www.technologyreview.com/2021/11/03/1039171/hackers-quantum-computers-us-homeland-security-cryptography/.

[16] Charles Griffiths, *The Latest 2024 Cyber Crime Statistics (Updated February 2024)*, AAG (Jan. 2, 2024), https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Headline%20Cyber%20Crime%20Statistics,the%20first%20half%20of%202022.

[17] O'Neill, *supra* note 15.

[18] *Id.*

[19] Marissa Norris, *Quantum Computers Will Break the Internet, but Only If We Let Them*, RAND (Apr. 9, 2020), https://www.rand.org/pubs/articles/2020/quantum-computers-will-break-the-internet-but-only-if-we-let-them.html.

### B. Cryptography

While it's predicted that quantum computers will gain functionality in the early to mid-2030s, the cybersecurity industry is racing to roll out new consumer data protection forms.[20] When consumers use the internet—i.e., using online banking or trading platforms—their data is generally secured by cryptography.[21] Contemporary cryptography employs sophisticated algorithms and ciphers to facilitate encryption, rendering consumer data unreadable to unauthorized parties, and decryption processes. Utilizing robust techniques such as 128-bit and 256-bit encryption keys, alongside modern ciphers like the Advanced Encryption Standard, ensures a level of security widely regarded as impervious to contemporary technological advancements.[22] FINRA noted in their report that "a hacker would need trillions of years using a conventional computer to break the encryption securing internet-based communication, such as a VPN."[23]

However, once deemed secure, the prevailing use of 128-bit and 256-bit encryption keys faces obsolescence within the next two decades due to the rise of sufficiently large quantum computers.[24] These quantum computers accelerate prime number factorization, rendering cryptographic keys, once considered computationally infeasible to crack, vulnerable to rapid compromise.[25] A report by RAND researchers that included interviews of academic and private sector cryptography experts suggested 2033 as the most likely year for creating a quantum

---

[20] *Id.*
[21] FORTINET, *What Is Cryptography?,* https://www.fortinet.com/resources/cyberglossary/what-is-cryptography (last visited Mar. 3, 2024).
[22] *Id.*
[23] Request for Comment, *supra* note 3.
[24] Gursimran Sethi, *Quantum Computing Will Breach Your Data Security*, MARSHMCLENNAN (Oct. 2022), https://www.marshmclennan.com/insights/publications/2022/october/quantum-computing-will-breach-your-data-security.html.
[25] *Id.*

computer that could break public-key cryptography.[26] This would be devastating because "[i]f hackers are ever able to crack public-key cryptography, then all information connected to the internet could be compromised."[27] Therefore, virtually all passwords, financial data, and assets are at risk of being stolen by hackers or nation-states.[28]

### C. Methods of Quantum Resistance

FINRA notes in its report that efforts are being made to respond to the threat that quantum computing poses.[29] Cyber security specialists are developing post-quantum cryptography (PQC) standards that could protect consumer data, and some experts predict that Congress will mandate PQC transition for government agencies, critical infrastructure, and other organizations.[30] Furthermore, the U.S., through the National Institute of Standards and Technology (NIST), has held a contest since 2016 that aims to produce the first quantum-computer-proof algorithms by this year.[31] As cryptography is the basis for securing more than 90 percent of internet-based connections—including that of our clients—FINRA is right to consider how the securities industry can reach a Fully Quantum-Safe Cryptographic State (FQSCS), where the data of our clients—and essentially the entire securities industry—cannot be stolen.[32]

### D. Conclusion

As FINRA considers offering guidance to its rules as it addresses the advent of quantum computing technology, we urge the agency to adopt PQC standards. We urge FINRA to take swift action on this issue, considering that the year 2033 is approaching, and the potential for

[26] Norris, *supra* note 19.
[27] *Id.*
[28] *Id.*; O'Neill, *supra* note 15.
[29] Request for Comment, *supra* note 3.
[30] O'Neill, *supra* note 15.
[31] *Id.*
[32] Request for Comment, *supra* note 3.

hackers to compromise public-key encryption, leading to the vulnerability of our clients' passwords, looms in the near future.[33]

## V. Quantum Computing Regulation

### A. Changing Risk Assessment Portfolios

The proliferation of quantum computing technology necessitates a comprehensive reevaluation of risk assessment strategies across the board for all investors. This rapid advancement may exacerbate issues associated with high-frequency trading (HFT), as discussed earlier in this comment.[34] Quantum computing, by significantly increasing processing speeds and computational capabilities, could intensify the challenges and risks already present in financial markets due to HFT.[35] These include market volatility, unfair competitive advantages, and the amplification of systemic risks. As quantum technology becomes more accessible, its impact on HFT and the broader financial sector requires careful consideration and regulation to mitigate potential negative consequences.

The Knight Capital incident on August 1, 2012, underlines the critical vulnerabilities and risks inherent in high-frequency trading and automated trading systems.[36] A software glitch following an update led to a catastrophic loss of approximately $440 million within just 45 minutes, pushing the firm to the brink of bankruptcy.[37] This event not only showcased the financial devastation caused by small software errors in the fast-paced world of HFT but also triggered a significant regulatory and industry-wide reevaluation of risk management practices

[33] Norris, *supra* note 19.
[34] *See supra* Section III.
[35] *See id.*
[36] *Regulator Fines Knight $12 Million Over Trading Error*, REUTERS (Oct. 16, 2013), https://www.reuters.com/article/idUSBRE99F12C/.
[37] *Id.*

and the implementation of more robust safeguards to prevent similar occurrences.[38] Knight Capital required emergency funding and an eventual merger with another firm to survive.[39] This highlights the importance of rigorous testing, robust risk management strategies, and the consideration of systemic risks posed by automated trading systems.[40] As a start reminder that risk assessment strategies must evolve and become more dynamic, it is imperative to reevaluate these approaches, incorporating comprehensive testing and validation processes to mitigate the inherent risks of sophisticated trading algorithms and systems.[41]

This reevaluation is driven by several transformative impacts of quantum computing on the financial sector:

- *Market prediction and analysis:* quantum computing's ability to process and analyze vast datasets far beyond the capability of classical computers can significantly enhance market prediction models.[42] This could lead to a deeper understanding of market trends and behaviors, prompting investors to adjust their risk assessment models to account for these more nuanced insights.[43] Institutional investors, with the resources to access quantum computing technologies, might gain unprecedented insights into market trends, risk factors, and investment opportunities.[44] This could lead to better-informed decisions and potentially higher returns with managed risks. For individual and smaller investors, the

[38] *See id.*
[39] Christina Rexrode & Pallavi Gogoi, *Cost of Glitch for Knight Capital: $440 Million*, AP WORLDSTREAM (Press Association, Inc. 2012), available at HighBeam Research (Aug. 5, 2012).
[40] *See also* In the Matter of Knight Capital Americas LLC, Administrative Proceeding, https://www.sec.gov/files/litigation/admin/2013/34-70694.pdf.
[41] Deloitte, *Managing Model Risk in Electronic Trading Algorithms: A Look at FMSB's Statement of Good Practice* (Mar. 23, 2023), https://www2.deloitte.com/uk/en/blog/auditandassurance/2023/managing-model-risk-in-electronic-trading-algorithms-a-look-at-fmsbs-statement-of-good-practice.html.
[42] *See supra* Section III.
[43] *How Quantum Computing Could Change Financial Services*, MCKINSEY & COMPANY (Dec. 18, 2020), https://www.mckinsey.com/industries/financial-services/our-insights/how-quantum-computing-could-change-financial-services.
[44] *Id.*

gap in accessing and leveraging such advanced analysis could widen, making it harder to compete on equal footing.[45]

- *Algorithmic trading:* the speeds at which quantum computers can execute complex trading algorithms could also dramatically change the landscape of algorithmic trading. This could lead to markets moving more quickly and unpredictably, requiring investors to reassess their strategies for mitigating risks associated with high-frequency trading and market volatility.[46] This could exacerbate market volatility and make it difficult for individual investors to time the market or react to price changes effectively, thus increasing the risk of losses.
- *Portfolio optimization*: quantum computing could allow for real-time portfolio optimization, considering a broader range of variables and scenarios than is currently feasible. This could change how investors assess the risk and return of different asset classes, potentially leading to more dynamic and responsive investment strategies. It could solve complex optimization problems more efficiently than classical computing.[47] Institutional investors could optimize their portfolios in real-time, dynamically adjusting to market changes to minimize risk and maximize returns. Individual and smaller investors, without access to such computational power, might find it challenging to maintain optimal portfolio allocations, potentially increasing their risk exposure.[48]
- *Regulatory and compliance risks:* as financial markets and institutions begin to integrate quantum computing; regulatory frameworks will need to evolve. Investors will have to navigate an evolving regulatory landscape, reassessing compliance risks and the impact

[45] *Id.*
[46] *See* Dylan Herman et. al., *Quantum Computing for Finance*, 5 NATURE REVIEWS PHYSICS 450 (2023).
[47] MCKINSEY & COMPANY, supra note 43.
[48] *Id*.

of new regulations on market dynamics and investment opportunities. Institutions might adapt more quickly to these changes, leveraging legal and compliance resources. Individual investors might struggle to keep up, facing increased legal and operational risks.

In response to these changes, risk assessment strategies will need to become more dynamic and adaptable. Investors may need to develop more sophisticated predictive models to understand market movements and consider new variables in their risk assessments.

**B. Risks of Market Manipulation and Disproportionate Impact on Smaller Investors**

The proliferation of quantum computing could increase the risk of market manipulation through high-frequency trading. The negative consequences could disproportionately impact smaller investors in several ways.

*1. Market Distortion and Manipulative HFT Practices can Distort True Market Conditions*

"Quote stuffing" may create a false sense of liquidity or market activity, while "layering" can falsely signal demand or supply shifts.[49] Smaller investors, relying on these distorted signals, may make trades based on misleading information, potentially leading to suboptimal investment decisions.[50]

- *Liquidity illusion:* large-scale HFT manipulative practices can create an illusion of liquidity in financial markets by rapidly placing and then canceling orders, a tactic designed to give the appearance of high trading activity without the intention of

[50] *See Manipulative Trading Practices: A Guide for Banks' Legal and Compliance Departments*, NORTON ROSE FULBRIGHT, November 2021, https://www.nortonrosefulbright.com/en/knowledge/publications/4a15661f/manipulative-trading-practices-a-guide-for-banks-legal-and-compliance-departments.

executing those trades.[51] This artificial liquidity, while making markets seem more active and robust under normal conditions, can vanish almost instantaneously when market volatility spikes or significant news events occur. In such scenarios, the rapid withdrawal of these superficial orders by high-frequency traders leads to a sudden and severe liquidity drought, leaving other market participants unable to execute trades at expected prices.[52] This phenomenon can exacerbate market movements, leading to increased volatility and potentially significant financial losses for investors who relied on what they believed was a liquid market. During periods of market stress, smaller investors who depend on this liquidity for trade execution may encounter challenges as the market becomes inundated with orders at unforeseen prices, potentially hindering their ability to execute trades.

- *Inflated market volatility:* by introducing a large volume of orders only to cancel them, these practices can contribute to increased volatility.[53] Smaller investors, who typically have less capital to buffer against sudden market movements, may find themselves at a disadvantage, as they may be less able to quickly adapt or absorb the costs of these fluctuations.
- *Cost implications:* manipulative HFT practices can cause smaller investors to enter or exit positions at non-optimal prices. This can result in higher transaction costs or lower returns than expected. Over time, these inefficiencies can erode the performance of investments for smaller investors.[54]

---

[51] Joseph Zabel, *Rethinking Open- and Cross-Market Manipulation Enforcement (August 27, 2020)*. 15 VA. L. & BUS. REV. 417, https://ssrn.com/abstract=3682103
[52] *Id*.
[53] *Id*.
[54] Ryan Wagner, *High Frequency Trading - Financial Ethics*, Seven Pillars Institute, https://sevenpillarsinstitute.org/case-studies/high-frequency-trading/.

*2. Lost Confidence in the Market*

The perception or reality of an uneven playing field can undermine confidence in the fairness and integrity of financial markets. Smaller investors may feel disadvantaged against HFT firms capable of manipulating market conditions, potentially leading to reduced participation or engagement with the market for small investors like those represented by our clinic.[55]

*3. Information Asymmetry*

HFT firms often have access to superior technology, data analysis tools, and direct market access. This technological edge can exacerbate information asymmetry, where smaller investors are operating with less information or at a slower pace, making it harder for them to compete on equal footing. [56]

**C. Potential Solution**

Collaborative efforts between technologists, financial analysts, regulatory bodies, and investors will be essential to navigate the challenges and opportunities presented by this groundbreaking technology. FINRA could take several proactive steps to ensure the integrity and stability of the markets, as well as to protect investors. Any action should also consider how these technologies evolve and are adopted within financial markets.[57]

*1. Updating Regulatory Frameworks*

FINRA could review and update its regulatory frameworks to address the new risks posed by quantum computing, particularly in areas like market manipulation, cybersecurity, and

[55] MCKINSEY & COMPANY, *supra* note 43.
[56] Dylan Herman et. al., *supra* note 46.
[57] FINRA, *About FINRA*, https://www.finra.org/about.

algorithmic trading.[58] This might include creating new rules or amending existing ones to cover the specific challenges quantum computing introduces.

*2. Monitoring and Surveillance Enhancements*

FINRA could invest in advanced monitoring and surveillance technologies capable of detecting the sophisticated trading patterns and potential manipulative practices that quantum computing might enable.[59] This could involve leveraging quantum computing itself to analyze market data more effectively.

*3. Educating Market Participants*

FINRA could initiate education and awareness programs for both investors and financial institutions about the potential impacts of quantum computing on financial markets. This could include guidance on risk management practices, cybersecurity measures, and compliance obligations.[60]

*4. Collaboration with Technological Experts*

To stay ahead of the curve, FINRA could collaborate with technology experts, including quantum computing specialists, to understand the evolving landscape and anticipate future challenges. This collaboration could inform regulatory strategies and the development of best practices for industry participants.[61]

*5. Facilitating Industry-Wide Discussions*

FINRA could organize forums and roundtable discussions involving a broad range of stakeholders, including financial institutions, technology companies, academics, and other

[58] *Id*.
[59] FINRA, *Technology*, https://www.finra.org/about/technology.
[60] FINRA, *supra* note 57.
[61] FINRA, *supra* note 59.

regulatory bodies. This could help with knowledge-sharing, identifying potential risks early, and developing industry-wide standards or responses to quantum computing challenges.[62]

*6. Risk Assessment and Management Guidance*

FINRA could provide guidance to firms on assessing and managing the risks associated with quantum computing. This could involve developing new risk assessment tools or methodologies that take into account the unique aspects of quantum technology.[63]

*7. Promoting Transparency and Fair Access*

To address concerns about market fairness and access disparities that quantum computing could exacerbate, FINRA could advocate for policies that promote transparency and equitable access to quantum computing resources for all market participants.[64] These policies aim to level the playing field for the unsophisticated investors we typically represent, seeking to hinder large financial firms from establishing technological or resource-based hegemony in the realm of quantum computing.

**D. Conclusion**

In the exploration of quantum computing's impact on the market, it's crucial to recognize the inherent disadvantages smaller investors face compared to large institutional investors. These disadvantages are primarily twofold: (1) limited access to advanced technology and (2) the difference in financial resources and risk tolerance.[65] Even when smaller and larger investors have similar technological capabilities, the vast resources of larger institutions enable them to engage in HFT strategies that compound upon and take advantage of market volatility.[66] This, in

[62] FINRA, *Requests for Comments*, https://www.finra.org/rules-guidance/requests-for-comments.
[63] FINRA, *supra* note 57.
[64] *Id*.
[65] *See supra* Section III; *see supra* Section V.A.
[66] MCKINSEY & COMPANY, *supra* note 43.

turn, pressures smaller investors into adopting suboptimal trading strategies.[67] Despite equal access to technology, the sheer scale of investment and risk management capabilities of larger firms places smaller investors at a disadvantage.

The SEC, under the Securities Act of 1933 and the Securities Exchange Act of 1934, possesses the authority to regulate market practices without directly controlling market volatility.[68] The SEC, therefore, has the jurisdiction to implement stricter regulations on HFT-related manipulations that contribute significantly to market volatility.[69] Techniques such as quote stuffing and layering, among others, could be more rigorously policed.[70]

Additionally, the SEC and FINRA should develop procedural rules leveraging quantum computing and artificial intelligence could empower regulatory bodies to more effectively identify, categorize, and mitigate the effects of manipulative HFT practices on the market. By utilizing advanced computing technologies, regulators could level the playing field, ensuring that the advantages of quantum computing do not disproportionately benefit those with the resources to exploit them.[71] This approach aims to safeguard market integrity and protect smaller investors from HFT volatility, thereby fostering a more equitable trading environment.[72]

Furthermore, quantum computing has the potential to impact the way options are priced. Options pricing involves complex mathematical models that require substantial computational resources. Quantum computing, with its advanced processing capabilities, can potentially enhance these calculations, leading to more accurate and faster pricing of options.[73] This could

---

[67] *See id.*
[68] *See* Securities Act of 1933, 15 U.S.C. §77a; Securities Exchange Act of 1934, 15 U.S.C. § 78a.
[69] *See id.*
[70] Zabel, Joseph, *supra* note 51.
[71] FINRA, *supra* note 59.
[72] *See* MCKINSEY & COMPANY, *supra* note 43.
[73] Nikitas Stamatopoulos et al., *Option Pricing Using Quantum Computers*, IBM Research (July 6, 2020), https://research.ibm.com/publications/option-pricing-using-quantum-computers.

have implications for the market, as more precise pricing might affect trading strategies and market dynamics.[74] Traders who take advantage of the improved computational power in option pricing, as long as they adhere to market rules and are not manipulative, typically remain within the bounds of accepted trading activities and are not specifically targeted by the SEC beyond its general oversight of securities markets.[75]

## VI. Conclusion

The University of Pittsburgh Securities Arbitration Clinic primarily serves a clientele comprised of elderly, economically disadvantaged, and unsophisticated investors—individuals particularly vulnerable to the potential risks posed by the swift advancements in quantum computing. High-frequency trading, inflated market volatility, and advanced decryption tools present risks to the small investor that a large firm has the tools to mitigate. FINRA, the SEC, and other bodies must provide protections through regulations and rule-making that protect these small investors. These include, but are not limited to, updating cryptographic and account security standards, customer education efforts, and risk management guidance. Proactive rulemaking in this field can minimize the risk of harm to investors and potentially limit future claims against financial institutions.

[74] *Id*.
[75] U.S. Securities and Exchange Commission, *The Laws That Govern the Securities Industry*, https://www.sec.gov/about/about-securities-laws; *see also* Securities Act of 1933, 15 U.S.C. §77a; Securities Exchange Act of 1934, 15 U.S.C. § 78a.