

The Legal Personhood of AI in the Financial Sector: Liability for Algorithmic Trading Losses

A Comparative Study of the United States and the European Union

Jolene Ren

Georgetown University

E-mail: jr2094@georgetown.edu

Published January 2026

Editor: Hayden Deschler, IE University

Abstract

Artificial intelligence now performs a substantial share of global financial trading, especially through autonomous high-frequency trading (HFT) systems. While these systems have improved liquidity and market efficiency, they have also produced systemic risks, including flash crashes and algorithmic manipulation. Traditional liability doctrines in financial regulation presuppose human intent, yet many trading algorithms operate with limited human oversight, generate unforeseeable strategies, and may cause widespread market disruptions absent any human intention. This paper asks whether autonomous trading algorithms should be treated as legal agents for the purpose of liability when their independent decisions cause economic harm.

The analysis compares the regulatory frameworks of the United States, particularly the Securities and Exchange Commission (SEC) regime, and the European Union's MiFID II and emerging AI Act. The U.S. system grounds liability in negligence, corporate responsibility, and enforcement targeting human actors, while the EU prioritizes ex ante risk-management, transparency, and technical safeguards. Through doctrinal analysis, case law, and scholarly debates on AI personhood, the paper evaluates whether either jurisdiction provides a coherent foundation for assigning responsibility to autonomous trading systems. The paper concludes with policy recommendations on how regulators might better address algorithmic autonomy without adopting full legal personhood for AI.

Keywords: autonomous trading algorithms, machine learning, systemic financial risk, legal accountability

1. Introduction

Artificial intelligence has steadily shifted from a back-end analytical tool in finance to an autonomous agent

executing trades with minimal human intervention.

High-frequency trading algorithms now account for the majority of daily transactions in U.S. equity markets and a

growing share in the European Union. These systems rely on machine-learning models that adapt to changing conditions, deploy complex strategies at millisecond speeds, and occasionally produce behaviours their developers did not anticipate. Such autonomy raises a central legal dilemma: when AI systems independently cause financial harm, who should bear liability?¹

This paper examines this dilemma through a comparative legal framework in order to answer whether high-frequency trading algorithms can be treated as autonomous agents under commercial law when their independent decisions cause large-scale market disruption. Existing legal frameworks in both the United States and the European Union assume that human actors—traders, broker-dealers, and risk managers—ultimately control the systems executing trades. Yet several events challenge this assumption: the 2010 Flash Crash, Knight Capital’s 2012 algorithmic malfunction, and episodes of AI-induced quote stuffing demonstrate that algorithms can destabilise markets absent any human intent.²

This paper argues that neither jurisdiction currently recognises AI personhood nor offers mechanisms sufficient to address the unique risks of autonomous algorithmic trading. Yet each system offers partial solutions. By comparing them, the paper proposes an improved liability framework grounded in enhanced oversight, mandatory auditability, and limited-purpose electronic

personhood—not for moral recognition, but to operationalise responsibility.³

2. Autonomous Trading and the Challenge to Traditional Liability Models

2.1 The Nature of Algorithmic Autonomy

Modern high-frequency trading systems combine machine-learning optimisation with pre-defined trading parameters. While humans design initial rules, the system identifies opportunities and executes strategies too quickly for human review. Scholars such as Hildebrandt and Pasquale argue that such systems exhibit operational autonomy, meaning the capacity to generate behaviour not explicitly programmed.⁴

This autonomy challenges traditional requirements for intent, knowledge, and mens rea in financial misconduct.

2.2 Systemic Risk and Unforeseeable Harm

Algorithmic malfunctions can cause cascading losses. Knight Capital’s trading glitch caused a USD 440 million loss within 45 minutes.⁵ The 2010 Flash Crash erased nearly USD 1 trillion in market value in minutes before partially rebounding.⁶ In both cases, regulators found no

¹ Mireille Hildebrandt, ‘Autonomous Systems and the Rule of Law’ (2019) *Technology and Regulation*.

² SEC and CFTC, ‘Findings Regarding the Market Events of May 6, 2010’ (2010).

³ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

⁴ Hildebrandt (n 1); Pasquale (n 3).

⁵ SEC, ‘Order Instituting Administrative and Cease-and-Desist Proceedings’ Exchange Act Release No 70694 (2013).

⁶ SEC and CFTC (n 2).

deliberate wrongdoing, only software failures interacting with market structure.

Traditional liability focuses on actors who cause harm, yet AI systems complicate causal attribution: was it the coder, the risk manager, or the algorithm acting according to its internal optimisation?

3. United States: Autonomous Trading and Traditional Liability Doctrine

3.1 SEC Approach: Human Accountability for Algorithmic Misconduct

The United States financial regulatory landscape is shaped primarily by the Securities Exchange Act, SEC enforcement actions, and self-regulatory organisations such as FINRA. United States law firmly rejects AI personhood: only natural persons and legal entities (corporations, partnerships) can bear liability. The SEC has not recognised algorithms as agents capable of intent.

Under United States doctrine, liability attaches to the entity deploying the algorithm. The SEC prosecutes misconduct under section 10(b) and Rule 10b-5, which require scienter—knowledge or recklessness.⁷ Courts have held that corporations can form intent through human employees, for example in *SEC v Citigroup Global Markets, Inc.*⁸ But algorithms cannot.

To address gaps, the SEC has proposed rules such as Regulation SCI, requiring systems integrity, and Market Access Rule 15c3-5, which mandates risk controls for automated trading.⁹ Enforcement actions such as *In re Athena Capital Research* show that regulators treat algorithms as tools deployed by humans, even when autonomous behaviour is central to the violation.¹⁰

3.2 Case Law Implicating Autonomous Systems

While there is no case directly granting agency status to AI, courts have begun recognising algorithmic opacity as a challenge. In *United States v Coscia*, a federal case involving spoofing, the court held that algorithms executing manipulative orders still reflected human intent because the programmer designed the strategy.¹¹

This reasoning becomes strained for self-learning or adaptive systems, which may produce strategies their developers never anticipated.

3.3 U.S. Policy Critique

The United States system is fundamentally reactive, relying on enforcement after harm occurs. It assumes human control and foreseeability—conditions that no longer describe machine-learning trading systems. Scholars have noted that negligence-based liability may be

⁷ Securities Exchange Act of 1934, s 10(b); 17 CFR § 240.10b-5.

⁸ *SEC v Citigroup Global Markets, Inc* 752 F.3d 285 (2d Cir 2014).

⁹ 17 CFR § 242.1000–1007; 17 CFR § 240.15c3-5.

¹⁰ *In re Athena Capital Research, LLC*, SEC Administrative Proceeding, Release No 9713 (2014).

¹¹ *United States v Coscia* 866 F.3d 782 (7th Cir 2017).

insufficient when harms stem from autonomous behaviour outside human foresight.¹²

Thus, the United States system leaves a responsibility gap: when no human satisfies scienter, liability under Rule 10b-5 may fail even if substantial harm occurred.

4. EU Approach: Procedural Accountability and Ex Ante Risk Controls

Unlike the United States' reliance on intent and scienter, the European Union grounds liability in procedural compliance under MiFID II, MiFIR, and the forthcoming EU Artificial Intelligence Act.¹³ These frameworks require firms deploying algorithmic trading systems to maintain pre-trade risk controls, circuit breakers, and throttling mechanisms, real-time monitoring, comprehensive internal audit trails, and detailed documentation of algorithmic parameters and updates.¹⁴

Regulators such as the European Securities and Markets Authority emphasise that harm may attach even absent human intent, so long as a firm violates mandated procedures or fails to implement adequate safeguards. This creates a stricter liability environment for algorithmic misconduct, particularly when firms cannot demonstrate compliance with risk-management obligations.

4.1 EU Case Law and Precedent Setting

While EU courts have not directly confronted AI personhood, administrative enforcement actions, such as BaFin's algorithmic trading sanctions, have consistently treated algorithmic failures as failures of supervisory procedure rather than human intent.¹⁵ This means liability can attach even where the algorithm's harmful behaviour was unforeseeable, expanding regulatory reach to emergent AI-driven harms.

5. Comparative Analysis: The Conceptual and Regulatory Gap

This section introduces the comparative framework and explains the analytical significance of the table below. The table clarifies how the United States and European Union differ in their assumptions about algorithmic autonomy, regulatory philosophy, and liability attribution. Presenting these contrasts in tabular form highlights structural gaps that doctrinal analysis alone may obscure.

5.1 Divergent Assumptions About Autonomy

Question	United States	European Union
----------	---------------	----------------

¹² Cary Coglianese and David Lehr, 'Regulating by Robot' (2017) Georgetown Law Journal.

¹³ Directive 2014/65/EU; Regulation (EU) No 600/2014.

¹⁴ ESMA, 'Guidelines on Systems and Controls in Algorithmic Trading' ESMA/2012/122.

¹⁵ BaFin, Algorithmic Trading Enforcement Action (public summaries).

Does the law assume human intent trades? Yes—central to liability. Less so; focuses on procedural safeguards.

Are algorithms considered independent actors? No. Algorithms are tools. No, but autonomy is indirectly acknowledged through risk categories.

Approach to regulation Ex post enforcement. Ex ante controls and documentation.

5.2 Points of Convergence

Both systems reject AI personhood, hold firms responsible for algorithmic behaviour, require kill-switches and supervisory controls, and recognise that autonomous trading poses systemic risks.

5.3 Points of Divergence

A first point of divergence concerns the treatment of unforeseeable autonomous behaviour. In the United States, if no human satisfies intent or negligence, liability may not attach. In the European Union, liability attaches

through violation of detailed procedural duties, even absent intent.

A second divergence relates to transparency and auditability. The United States imposes limited auditability requirements for source code, for example through the SEC’s Consolidated Audit Trail system.¹⁶ By contrast, the European Union imposes strong legal requirements under MiFID II and the Artificial Intelligence Act.

A final divergence lies in regulatory philosophy. The United States relies on market discipline combined with enforcement, whereas the European Union adopts a precautionary principle combined with structured oversight.

5.4 Do Either Jurisdiction Provide a Basis for AI Personhood?

Neither provides a doctrinal basis for recognising algorithms as legal persons. The United States could theoretically adapt corporate personhood frameworks to create algorithmic entities, but no movement in Congress or the courts supports such a change. The European Union briefly considered limited electronic personhood for autonomous systems in 2017, but Parliament ultimately rejected the proposal.¹⁷

¹⁶ Securities Exchange Act Release No 79318 (2016).

¹⁷ European Parliament, ‘Civil Law Rules on Robotics’ Resolution 2015/2103(INL).

Thus, both systems address AI as a compliance object, not a liability subject. The responsibility gap remains unresolved.

6. Counterarguments

6.1 AI Personhood Is Conceptually Flawed

Critics argue that personhood is inappropriate because AI lacks consciousness and moral agency.¹⁸ Corporate personhood, however, does not require consciousness. The relevant question is functional: can personhood facilitate liability assignment?

6.2 Firms Will Evade Responsibility by Offloading Blame to AI

This concern is valid; granting independent legal status to algorithms may encourage firms to treat the AI as a judgment-proof shell. Any AI personhood regime would therefore require joint liability with deploying firms.

6.3 Enhanced Human Oversight Is Enough

Some scholars argue that autonomy is overstated and that better testing and supervision suffice.¹⁹ Yet emergent algorithmic behaviours, such as reinforcement-learning strategies evolving in unpredictable ways, suggest that full oversight is infeasible.

7. Policy Recommendation

This section proposes a hybrid model blending insights from the United States and European Union regimes. A blended model requires adapting United States post hoc enforcement to incorporate the European Union's preventative safeguards. Regulators should require firms to formally classify each trading algorithm by risk level, maintain updated model cards describing decision logic, and provide regulators with continuous access to audit data.

7.1 Rationale for Hybrid Approach

Because high-frequency trading systems operate across borders and millisecond timescales, national regimes alone cannot effectively address systemic risk. Harmonised standards would reduce regulatory arbitrage, improve market stability, and ensure consistent treatment of algorithmic decision-making.

7.2 Establishing Limited Electronic Personhood for HFT Algorithms

This would not constitute moral personhood but functional legal status enabling attribution of algorithmic decisions, mandatory registration, and insurable liability. The entity would be jointly and severally liable with the deploying firm, preventing externalisation of risk.

7.3 Algorithmic Audit Trails and Explainability

¹⁸ Ryan Calo, 'Robotics and the Lessons of Cyberlaw' (2015) California Law Review.

¹⁹ Brent Mittelstadt and others, 'The Ethics of Algorithms' (2016) Big Data & Society.

Borrowing from the Artificial Intelligence Act, both jurisdictions should mandate immutable trading logs, explainability reports for regulators, and independent audit authority access to model parameters.

7.4 Market-Wide Algorithmic Stress Tests

Similar to bank stress tests, regulators should require simulation of extreme market conditions, evaluation of algorithmic interactions, and mandatory pre-deployment certification.

7.5 Expanding Strict Liability Regimes

For damage caused by autonomous trading, regulators should impose strict liability on firms unless they can prove compliance with enhanced procedural safeguards.

7.6 Harmonising U.S.–EU Regulatory Cooperation

Given cross-border trading, regulators should establish common audit standards, share data on algorithmic incidents, and coordinate enforcement to prevent regulatory arbitrage.

8. Conclusion

Autonomous trading systems challenge foundational assumptions in financial law. As algorithms increasingly make high-speed decisions beyond human foresight, traditional liability doctrines tied to human intent and corporate negligence become inadequate. The United States' reliance on ex post enforcement and scienter-based

liability leaves gaps when AI behaviour is unintentional and emergent. The European Union's ex ante procedural protections reduce some risks but still struggle with unforeseeable algorithmic harms. Neither system currently offers a coherent pathway for assigning responsibility to autonomous trading algorithms themselves.

This paper argues for a limited form of electronic personhood, strictly functional rather than moral, combined with enhanced auditability, strict liability, and cross-border regulatory harmonisation. Such reforms would not absolve firms of responsibility; rather, they would enable regulators to map causal pathways, allocate liability fairly, and ensure that autonomous systems do not undermine market integrity. As financial markets continue integrating AI, legal frameworks must evolve to ensure accountability, systemic stability, and public trust.

Bibliography

U.S. Legal & Regulatory Sources

Consolidated Audit Trail (CAT) NMS Plan
Securities Exchange Act Release No 79318 (2016).

Securities Exchange Act of 1934
15 USC § 78a et seq.

SEC Market Access Rule (Rule 15c3-5)
17 CFR § 240.15c3-5.

SEC Regulation SCI
17 CFR § 242.1000–1007.

SEC Rule 10b-5
17 CFR § 240.10b-5.

U.S. Case Law

In re Athena Capital Research, LLC
SEC Administrative Proceeding, Release No 9713
(Oct 2014).

SEC v Citigroup Global Markets, Inc
752 F.3d 285 (2d Cir 2014).

United States v Coscia
866 F.3d 782 (7th Cir 2017).
(Spoofing, algorithmic trading; important for intent
analysis)

U.S. Market Events & Official Reports

Knight Capital Group Trading Glitch
SEC, ‘Order Instituting Administrative and
Cease-and-Desist Proceedings’
Exchange Act Release No 70694 (Oct 2013).

SEC & CFTC Joint Staff Report on the 2010 Flash Crash
‘Findings Regarding the Market Events of May 6,
2010’ (Sept 2010).

European Union Law

Artificial Intelligence Act (EU)
Interinstitutional File 2021/0106(COD).
(As politically agreed between Council and Parliament)

Markets in Financial Instruments Directive II (MiFID II)
Directive 2014/65/EU.

Markets in Financial Instruments Regulation (MiFIR)
Regulation (EU) No 600/2014.

EU Regulatory Guidance & Enforcement

BaFin (German Federal Financial Supervisory Authority)
Algorithmic Trading Enforcement Action
BaFin administrative sanctions regarding HFT
controls (public summaries).

ESMA (European Securities and Markets Authority)
Guidelines on Systems and Controls in Algorithmic
Trading
ESMA/2012/122.

Academic and Scholarly Sources

Awrey D, ‘Regulating Systemic Risk in Financial Markets’
(2013) *Oxford Journal of Legal Studies*.
(Used to support systemic risk discussion)

Balkin J, ‘The Path of Robotics Law’ (2015) *California
Law Review*.
(On governance gaps)

Bloch-Wehba H, ‘Algorithmic Accountability:
Technical/Legal Standards’ (2020) *Fordham Law
Review*.
(On oversight limits)

Calo R, ‘Robotics and the Lessons of Cyberlaw’ (2015)
California Law Review.
(On personhood and responsibility gaps)

Coglianesi C and Lehr D, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) *Georgetown Law Journal*.

(On foreseeability and algorithmic behaviour)

Hildebrandt M, 'Autonomous Systems and the Rule of Law' (2019) *Technology and Regulation*.

(On operational autonomy)

Mittelstadt B and others, 'The Ethics of Algorithms' (2016) *Big Data & Society*.

(Used for autonomy/opacity principles)

Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

(On opacity and algorithmic unpredictability)

European Parliament, 'Civil Law Rules on Robotics' Resolution 2015/2103(INL).

(Rejected proposal for electronic personhood)

Technical & Industry Sources

BIS (Bank for International Settlements), 'Algorithmic Trading in Financial Markets' BIS Papers No 165 (2022).
(Background empirical data)

Nanex Data (Eric Hunsader)
High-frequency trading quote stuffing and Flash Crash pattern analysis.
(Frequently cited in academic literature)

OECD,
'AI in Finance: Risks and Regulatory Responses' (2021).
(Policy framing)