Volume 10, No. 1 | January-February 2027

RAIL

The Journal of Robotics, Artificial Intelligence & Law

Editor's Note: Contrasting Strategies
Victoria Prussen Spears

AI, Intellectual Property, and National Security: Understanding the Administration's Contrasting Strategies
Armin Ghiam and Andre Earls

The Evolving AI Patchwork: Balancing U.S. State Shifts and EU Mandates in Deal Negotiations
David A. Toy, Thomas J. Petrie, and Colin Harris

Adapting Error Resolution to Agentic AI Payments
David A. Stein

AI Is Making Phishing Scams Almost Impossible to Spot—5 Steps Employers Should Take to Combat Latest Threat
Daniel Pepper and Michael Steele

Indian Gaming and Prediction Markets: On a Collision Course?
Blaine I. Green and Allan C. Van Vliet

Prediction Markets Are Creating a New Insider Trading Frontier for Biotech and Pharmaceutical Companies
Chelsea Anderson and Noah Solowiejczyk

CFTC Targets George Santos for Manipulative Trading in State of the Union Event Contract
John C. Murphy, Katherine R. Goldstein, James Joseph Benjamin Jr., Michael A. Asaro, Peter I. Altman, Parvin Daphne Moyne, and Lance Jasper

Different Shoppers, Different Prices: The Federal Trade Commission Takes Aim at Personalized Pricing
Allyson L. Chavez, Anna M. Behrmann, and Kathy L. Osborn

Third Circuit Revives Algorithmic Price-Fixing Suit Against Atlantic City Hotels
Alexis Gilman and Drew Wilson

Model Cloning of a Competitor's AI: Fair Competition or Potential Liability?
Brian W. Nolan, Reginald R. Goeke, Adam S. Hickey, Thea Kendler, and Micheal Antifaoff

Automating the Impact Assessment, and the Limits of AI Compliance
Adilson Fernandes Braga Junior

The UK ICO's New Statutory Duty to Produce an AI Code of Practice: What It Means for Businesses That Use AI
James Castro-Edwards

FULL COURT PRESS
part of Clio

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 10, No. 1 | January–February 2027

7 **Editor's Note: Contrasting Strategies**
Victoria Prussen Spears

11 **AI, Intellectual Property, and National Security: Understanding the Administration's Contrasting Strategies**
Armin Ghiam and Andre Earls

17 **The Evolving AI Patchwork: Balancing U.S. State Shifts and EU Mandates in Deal Negotiations**
David A. Toy, Thomas J. Petrie, and Colin Harris

23 **Adapting Error Resolution to Agentic AI Payments**
David A. Stein

33 **AI Is Making Phishing Scams Almost Impossible to Spot—5 Steps Employers Should Take to Combat Latest Threat**
Daniel Pepper and Michael Steele

37 **Indian Gaming and Prediction Markets: On a Collision Course?**
Blaine I. Green and Allan C. Van Vliet

43 **Prediction Markets Are Creating a New Insider Trading Frontier for Biotech and Pharmaceutical Companies**
Chelsea Anderson and Noah Solowiejczyk

49 **CFTC Targets George Santos for Manipulative Trading in State of the Union Event Contract**
John C. Murphy, Katherine R. Goldstein, James Joseph Benjamin Jr., Michael A. Asaro, Peter I. Altman, Parvin Daphne Moyne, and Lance Jasper

55 **Different Shoppers, Different Prices: The Federal Trade Commission Takes Aim at Personalized Pricing**
Allyson L. Chavez, Anna M. Behrmann, and Kathy L. Osborn

61 **Third Circuit Revives Algorithmic Price-Fixing Suit Against Atlantic City Hotels**
Alexis Gilman and Drew Wilson

67 **Model Cloning of a Competitor's AI: Fair Competition or Potential Liability?**
Brian W. Nolan, Reginald R. Goeke, Adam S. Hickey, Thea Kendler, and Micheal Antifaoff

75 **Automating the Impact Assessment, and the Limits of AI Compliance**
Adilson Fernandes Braga Junior

85 **The UK ICO's New Statutory Duty to Produce an AI Code of Practice: What It Means for Businesses That Use AI**
James Castro-Edwards

Adapting Error Resolution to Agentic AI Payments

David A. Stein*

In this article, the author explains that autonomous payments initiated by artificial intelligence (AI) agents on behalf of consumers raise substantial payments law issues, including how and by whom alleged unauthorized or erroneous transfers should be investigated and resolved. Agentic AI payments, the author adds, also prompt questions about the adequacy of existing consumer dispute provisions and the risk of repeating what happened with the growth of peer-to-peer payments—high volumes of consumer disputes alleging unauthorized transactions, regulatory actions, litigation, and political backlash. The author then identifies specific areas where targeted regulatory updates may create a better experience for all parties, focusing on Electronic Fund Transfer Act/Regulation E and ACH transactions.

Background

Agentic artificial intelligence (AI) payment applications allow consumers to delegate to an AI agent authority to make purchases and initiate payments from a consumer's account without the consumer's active participation. The consumer defines the parameters of the AI agent's authority and gives the agent discretion within those parameters to initiate payments autonomously. A consumer may delegate authority to shop for and purchase goods or services at merchants, manage subscriptions and recurring payments, or transfer funds between accounts for financial management purposes.

When using agentic AI payments, the consumer may provide his or her access device, such as bank account login credentials or similar information, to the provider of the agentic AI payment application (Agentic Payment Provider) so the AI agent can initiate transactions from the consumer's bank account. Alternatively, the consumer may grant authority through technological means that do not require the consumer to share an access device. The latter approach presumably would involve an agreement between the consumer's account-holding institution and the Agentic Payment Provider.

Consumers will dispute agentic AI payment transactions for various reasons. Consumer instructions to an AI agent may be

Robotics, Artificial Intelligence & Law / January-February 2027, Vol. 10, No. 1, pp. 23-31
© 2027 Full Court Press. All rights reserved
ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

imprecise, resulting in unwanted purchases. An AI agent may initiate transactions in excess of specified limits on its authority, for example, stated dollar or time limits, or merchant or product restrictions. An AI agent also may be targeted by scams and tricked into conducting transactions with fictitious merchants, be taken over and exploited by malicious actors, or even be created by fraudsters.

Assumptions

This article makes the following assumptions. First, the Agentic Payment Provider will not be the consumer's account-holding institution or its service provider. While financial institutions, or a consortium of financial institutions, may offer agentic AI payments, history suggests that non-bank fintechs may be early movers in agentic AI payments.

Second, agentic AI payment applications will use multiple payment rails, including ACH (Automated Clearing House) and possibly cryptocurrency rails. Although payment card networks proactively amended their rules to address agentic AI payments made using credit and debit cards, there is no guaranty that agentic AI payments will use the credit card and debit card rails. Merchants may prefer ACH-based agentic AI payments to avoid interchange fees and chargeback obligations, while non-bank Agentic Payment Providers may balk at complying with card network rules.

Third, financial institutions and fintechs will seek to hold consumers responsible for allegedly unauthorized payment transactions initiated autonomously by AI agents, including when AI agents exceed specified limits on their authority or are tricked into paying fictitious merchants.

Unauthorized EFT Analysis

Definitions and Scope

Unauthorized EFT and Unauthorized Use Definitions

An "unauthorized electronic fund transfer" means "an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the

transfer and from which the consumer receives no benefit."[1] The term excludes an EFT initiated "by a person who was furnished the access device to the consumer's account by the consumer, unless the consumer has notified the financial institution that transfers by that person are not longer authorized."[2]

Under Regulation Z, "unauthorized use" means "the use of a credit card by a person, other than the cardholder, who does not have actual, implied, or apparent authority for such use, and from which the cardholder receives no benefit."[3]

Although the two definitions are similar, the Electronic Fund Transfer Act (EFTA) and Regulation E require an unauthorized EFT to be made by a person "without *actual* authority," whereas Regulation Z provides that unauthorized use of a credit card includes use by a person who lacks "*actual*, *implied*, or *apparent* authority for such use."

Actual Authority

Agentic AI payments, by design, give AI agents discretion to make autonomous purchase/payment choices and involve a trade-off between precise consumer instructions and agent discretion to act on the consumer's behalf without active consumer engagement. Factual questions inevitably will arise regarding an AI agent's authority to initiate a disputed transaction. The absence of "implied" and "apparent" authority language in the EFTA and Regulation E could make it more difficult to resolve such disputes under the "actual authority" standard than under Regulation Z's "actual, implied, or apparent authority" standard.

No Consumer Benefit

The consumer must "receive[] no benefit" from an unauthorized EFT. If a merchant delivers the purchased goods or services to the consumer, the consumer receives a benefit, even if the consumer does not want the goods or services. Also relevant is whether the consumer did not or could not return the goods or services to the merchant for a refund.

AI Agent Characterization

A key issue is whether an EFT initiated by an AI agent is deemed an act of the consumer or is "initiated by a person other

than the consumer." Neither the EFTA nor Regulation E address this question.

The EFTA and Regulation E define a "consumer" to mean "a natural person,"[4] while a "person" includes both natural persons and organizations.[5] Based on these definitions, a regulator or court may find that an AI agent is not and cannot be a "natural person," even when acting on a consumer's behalf. The Agentic Payment Provider presumably will not be a "natural person." Thus, the AI agent and/or the Agentic Payment Provider may be deemed "a person other than the consumer" under the unauthorized EFT definition when the agent initiates EFTs on the consumer's behalf. This conclusion is not certain, however. While the Restatement (Third) of Agency provides that a principal and an agent are not the same person,[6] other relevant authority suggests that an electronic agent is simply a tool employed by the consumer using it with the consumer responsible for the results.[7]

An AI agent's characterization has implications for disputes. If the AI agent is the consumer's agent, "a person other than the consumer," its authority and the furnished access device exclusion remain relevant for resolving unauthorized EFT claims. If the AI agent and the consumer are the same person, the only unauthorized EFTs will involve loss or theft of an access device, for example, where a third party fraudulently obtains an access device from an AI agent. The furnished access device exclusion is inapplicable if the consumer and AI agent are the same "person" because the consumer does not furnish an access device to another person.

Furnished Access Device Exclusion

The furnished access device exclusion may apply where the AI agent is the consumer's agent. If the consumer furnishes an access device and grants the AI agent authority to initiate payments using the device, the consumer's account-holding institution will consider the resulting transactions authorized, unless the consumer has notified the institution to revoke the AI agent's authority. And revocation is unlikely until the AI agent initiates transactions the consumer claims were unauthorized. The institution will maintain that furnishing an access device and granting EFT authority to an AI agent is no different than furnishing an access device and granting EFT authority to a family member or co-worker, each of

whom exceeds their authority. The text of Regulation E supports this position. Consumers nonetheless will assert that EFTs initiated in excess of the AI agent's authority are unauthorized.

Existing Error Resolution Framework

Under Regulation E, a "financial institution" means a person that holds a consumer's account or that issues an access device and agrees with a consumer to provide EFT services.[8] If multiple financial institutions participate in a single EFT, each must investigate alleged errors even if another institution would have the same obligations if notified by the consumer.

A "service provider" is a person that provides an EFT service to a consumer but does not hold the consumer's account if the person: (1) issues an access device the consumer can use to access the consumer's account held by a financial institution; and (2) has no agreement with the account-holding institution regarding such access.[9] When a service provider participates in a transaction, the service provider, not the account-holding institution, is subject to Regulation E's error resolution requirements.[10] In other words, only one party—the service provider—must investigate consumer disputes.

Under Regulation E, a financial institution satisfies its duty to investigate alleged errors by conducting a review of *its own records* if: (1) the alleged error concerns a transfer to or from a third party; and (2) there is no agreement between the institution and the third party for the type of EFT involved,[11] known as the "four walls" rule. A financial institution's participation in transactions cleared through an ACH network is not an agreement, meaning investigations of disputed ACH transactions can be based on the institution's own records (including any information submitted by the consumer).[12] In contrast, a financial institution's obligation to honor an access device, such as a debit card issued by another person, under payment card network rules is an agreement under Regulation E's error resolution provisions, and the investigation cannot be limited to the institution's own records.[13] Thus, the scope of an error resolution investigation differs for debit card and ACH transactions.

Application to Agentic AI Payments

Applying the existing error resolution framework to agentic AI payments raises several issues. First, it is unknown if Agentic Payment Providers will issue access devices or hold consumer accounts, consider themselves "financial institution(s)" or service providers, afford consumers error resolution rights, or execute agreements with account-holding institutions. Experience with prior innovations suggests: (1) Agentic Payment Providers will prefer to avoid Regulation E error resolution obligations given the cost of providing provisional credits and making consumers whole; (2) consumers will submit disputes to account-holding institutions about agentic AI payments; and (3) inter-party agreements may be slow to gain traction but could prohibit Agentic Payment Providers from obtaining access devices and require them to conduct or cooperate with error resolution investigations.

Second, giving consumers the choice of asserting disputes with any financial institution involved in an ACH transaction—whether the account-holding institution or an access device issuer—sounds good in theory. In practice, this approach has proven less than satisfactory. One reason is the financial institution not receiving the consumer's dispute notice has no obligation and little incentive to share information with the institution investigating the dispute. If the consumer submits disputes to both institution, each may satisfy its obligations by reviewing information within "its own records." Two compliant investigations each based on incomplete information.

Third, applying the "four walls" rule to agentic AI payment disputes creates problems because information about the AI agent's authority and conduct will not be within the account-holding institution's own records. This lack of visibility into the AI agent's authority and conduct will make it difficult for account-holding institutions to confirm or disprove consumer claims of lack of authority and to investigate disputes alleging fraud perpetrated by or against an AI agent. External information about AI agents' authority and conduct is critical for these purposes. The results could frustrate financial institutions and consumers alike, raise doubts about the safety and reliability of agentic AI payments, and prove reminiscent of the peer-to-peer (P2P) payments experience with high volumes of disputes, regulatory actions, litigation, and

political backlash. There is a more constructive way to approach agentic AI payment disputes.

Reconsidering the Four Walls Rule

The emergence of complex, multi-party ACH transactions, such as agentic AI payments and P2P payments, calls into question continued reliance on the "four walls" rule. The rule looks increasingly anachronistic in the context of newer forms of EFTs and the types of disputes they will generate. When financial institutions do not possess, and cannot obtain from other participants, information relevant for resolving unauthorized EFT claims, the resulting investigations, through no fault of the investigating institution, can have evidentiary shortcomings that undermine the credibility of the error resolution process.

Regulation E's service provider provision takes a different approach. It requires the service provider to assume all error resolution obligations, except that, upon request, the account-holding institution must provide the service provider with information it needs to investigate the alleged errors.[14] By requiring an entity exempt from error resolution obligations to share necessary information, upon request, with the entity conducting the investigation, this provision effectively supersedes the "four walls" rule.

Applying a version of the service provider information-sharing provision to agentic AI payment disputes is a regulatory change worth considering. Such a provision would serve three goals:

1. To move beyond the "four walls" rule and "its own records" approach to error resolution investigations, which fails to account adequately for complex, multi-party ACH transactions;
2. To bring investigations of ACH disputes more in line with investigations of debit card disputes and reduce opportunities for regulatory arbitrage across payment rails; and
3. To give financial institutions investigating consumer disputes timely access to more complete information so they can fully investigate and fairly resolve agentic AI payment disputes in a way that lends credibility to the error resolution process. Better information about disputed transactions and AI agents' authority and conduct,

facilitated by a well-crafted information-sharing obligation, should result in more thorough investigations, defensible outcomes, and reduced litigation and enforcement risk.

An information-sharing rule, however, need not assign error resolution responsibility to just one party. Instead, a reciprocal information-sharing rule could require both the Agentic Payment Provider and account-holding institution to provide relevant information to the other party, upon request, when the other party is investigating a consumer dispute, subject to appropriate verification and data security measures.

Enhanced information sharing also does not mean consumers will prevail. Shared information may demonstrate the consumer authorized payment, the AI agent acted within its authority, or the furnished access device exclusion applies. In such cases, Regulation E will not afford consumers relief. Regulation E, however, is not and should not be a cure-all for all consumer payments issues. Consumers may have other avenues of redress, including by attempting to resolve the issue with merchants via returns and refunds, or by pursuing the Agentic Payment Provider for state law claims if the AI agent exceeds its authority or is compromised by malicious actors.

Conclusion

Agentic AI payments are the leading edge of payments innovation and will develop in unforeseen ways. Still, it is not too soon to identify regulatory gaps and reconsider provisions not suitable for agentic AI payments. Certain questions—whether an Agentic Payment Provider is a "financial institution" or a service provider, or what constitutes a grant of "actual authority" to an AI agent—may not be ripe for resolution. Other questions, including whether an AI agent is the consumer or a "person other than the consumer," may require earlier attention. The "four walls" rule, in particular, is inadequate for consumer disputes financial institutions increasingly encounter with complex, multi-party ACH payments. Thus, while much can and should be left to market developments and industry-led standard setting to guide agentic AI payment development, targeted regulatory updates will be necessary. Reconsideration of Regulation E's "four walls" rule is a good place to begin.

Notes

* The author, of counsel to Covington & Burling LLP, may be contacted at dstein@cov.com.

1. 15 U.S.C. § 1693a(12); 12 C.F.R. § 1005.2(m).
2. 12 C.F.R. § 1005.2(m) (hereafter the furnished access device exclusion); see also 15 U.S.C. § 1693a(12).
3. 12 C.F.R. § 1026.12(b)(1)(i).
4. 15 U.S.C. § 1693a(6); 12 C.F.R. § 1005.2(e).
5. 12 C.F.R. § 1005.2(j).
6. Restatement (Third) of Agency, § 1.01 ("Agency is the fiduciary relationship that arises when one person (a "principal") manifests assent to another person (an "agent") that the agent shall act on the principal's behalf and subject to the principal's control, and the agent manifests assent or otherwise consents to so act.").
7. See Uniform Electronic Transactions Act § 2(6) cmt. (1999) (an electronic agent employed by a person "is a tool of that person" and the person using the tool is responsible for its results since the tool "has no independent volition of its own[,]" but noting that "within the useful life of this Act, electronic agents may be created with the ability to act autonomously, not just automatically."); Visa Rules, §§ 4.1.24.3, 4.1.24.10, and Glossary (Definitions of "Agent," "Agentic Payment Provider," "Agentic Transaction," and "Cardholder") (Apr. 18, 2026) (an Agentic Payment Provider to a Cardholder is considered the Cardholder, not an Agent, for an Agentic Transaction undertaken on a Cardholder's behalf using a payment credential).
8. 12 C.F.R. § 1005.2(i).
9. 12 C.F.R. § 1005.14(a).
10. 12 C.F.R. §§ 1005.14(b)(2) and (c).
11. 12 C.F.R. § 1005.11(c)(4). The third party is the person to whom funds are transferred, for example, the merchant.
12. 12 C.F.R. Part 1005, Comment § 1005.11(c)(4)-4.
13. Id.
14. 12 C.F.R. § 1005.14(c)(2).

EDITOR-IN-CHIEF

Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Jennifer A. Johnson
Partner, Covington & Burling LLP

Paul B. Keller
Partner, Allen & Overy LLP

Garry G. Mathiason
Shareholder, Littler Mendelson P.C.

James A. Sherer
Partner, Baker & Hostetler LLP

Elaine D. Solomon
Partner, Blank Rome LLP

Edward J. Walters
Chief Strategy Officer, vLex

John Frank Weaver
Director, McLane Middleton, Professional Association

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, an imprint of Clio and Themis Solutions, Inc..
Copyright 2027 Full Court Press, an imprint of Clio and Themis Solutions, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Full Court Press, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: David Nayer
Production Editor: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Full Court Press)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2027 Full Court Press, an imprint of Clio and Themis Solutions, Inc.

All Rights Reserved.

A Full Court Press, Clio, Publication

https://www.fastcase.com/

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

David Nayer, Publisher, Full Court Press at david.nayer@clio.com or at 202.999.4777

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2575-5633 (print)
ISSN 2575-5617 (online)