Volume 7, No. 2 | March–April 2024

The Journal of Robotics, Artificial Intelligence & Law

Editor's Note: AI Regulation Is Becoming Global Now
Victoria Prussen Spears

G7 Leaders Publish AI Code of Conduct: A Common Thread in the Patchwork of Emerging AI Regulations Globally?
Henry Mostyn, Gareth Kristensen, Ferdisha Snagg, Prudence Buckland, and Andreas Wildner

Artificial Intelligence in the Financial Services Sector: UK Regulators Publish Feedback Statement
Ferdisha Snagg and Andreas Wildner

Legislative Responses to Recent Developments in Generative Artificial Intelligence
Christopher A. Bloom, Corey Bieber, Austin D. McCarty, and Scott J. Gelbman

Court Dismisses Algorithmic Price-Fixing Case, But Opens Door to Amended Complaint
Alexis J. Gilman, Jordan Ludwig, Jeane A. Thomas, and Darianne Young

California Announces Privacy Audits of Connected Vehicles and Related Technologies
Steven G. Stransky, Thomas F. Zych, Marla M. Izbicky, and Thora Knight

The CHIPS and Science Act of 2022 and the Emerging Intellectual Property Landscape
T.J. Clark and Shane Hunter

Boardroom Cryptonite: Assessing Coverage for Crypto-Related Exposures
Michael S. Levine, Geoffrey B. Fehling, Lorelie S. Masters, and Yaniel Abreu

Risks and Mitigation of Bias in Medical AI
Judd Chamaa and Zach Harned

Protecting Brands in the Age of AI
Paul Famiglietti and Connie L. Ellerbach

AI in M&A: 10 Things to Consider in Acquisitions
Julia Apostle, Alexis Marraud des Grottes, and Zac Padgett

Start-Up Corner: I Have a Company That Was Formed in Another Country, But I Want to Set Up a Delaware C Corporation for VC Investors. How Do I Process and Structure Something Like That?
Christopher C. McKinnon, Jim Ryan, and Scott Perlov

Start-Up Corner: Buying Certainty in an Uncertain World Through Litigation Risk Insurance
Kevin V. Small, Patrick M. McDermott, and Alex D. Pappas

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 7, No. 2 | March–April 2024

95 **Editor's Note: AI Regulation Is Becoming Global Now**
Victoria Prussen Spears

99 **G7 Leaders Publish AI Code of Conduct: A Common Thread in the Patchwork of Emerging AI Regulations Globally?**
Henry Mostyn, Gareth Kristensen, Ferdisha Snagg, Prudence Buckland, and Andreas Wildner

107 **Artificial Intelligence in the Financial Services Sector: UK Regulators Publish Feedback Statement**
Ferdisha Snagg and Andreas Wildner

113 **Legislative Responses to Recent Developments in Generative Artificial Intelligence**
Christopher A. Bloom, Corey Bieber, Austin D. McCarty, and Scott J. Gelbman

121 **Court Dismisses Algorithmic Price-Fixing Case, But Opens Door to Amended Complaint**
Alexis J. Gilman, Jordan Ludwig, Jeane A. Thomas, and Darianne Young

125 **California Announces Privacy Audits of Connected Vehicles and Related Technologies**
Steven G. Stransky, Thomas F. Zych, Marla M. Izbicky, and Thora Knight

129 **The CHIPS and Science Act of 2022 and the Emerging Intellectual Property Landscape**
T.J. Clark and Shane Hunter

133 **Boardroom Cryptonite: Assessing Coverage for Crypto-Related Exposures**
Michael S. Levine, Geoffrey B. Fehling, Lorelie S. Masters, and Yaniel Abreu

141 **Risks and Mitigation of Bias in Medical AI**
Judd Chamaa and Zach Harned

149 **Protecting Brands in the Age of AI**
Paul Famiglietti and Connie L. Ellerbach

153 **AI in M&A: 10 Things to Consider in Acquisitions**
Julia Apostle, Alexis Marraud des Grottes, and Zac Padgett

Start-Up Corner

159 **I Have a Company That Was Formed in Another Country, But I Want to Set Up a Delaware C Corporation for VC Investors. How Do I Process and Structure Something Like That?**
Christopher C. McKinnon, Jim Ryan, and Scott Perlov

163 **Buying Certainty in an Uncertain World Through Litigation Risk Insurance**
Kevin V. Small, Patrick M. McDermott, and Alex D. Pappas

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, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

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:

Morgan Morrissette Wright, Publisher, Full Court Press at morgan.wright@vlex.com or at 202.999.4878

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)

Boardroom Cryptonite: Assessing Coverage for Crypto-Related Exposures

Michael S. Levine, Geoffrey B. Fehling, Lorelie S. Masters, and Yaniel Abreu*

In this article, the authors address potential insurance coverage for crypto losses under various types of insurance policies and how to deal with insurers that reject crypto claims, as well as precautionary steps that companies and their executives can take to preempt, or alternatively to address, a denial of coverage.

The collapse of cryptocurrencies and some exchanges and the recent Securities and Exchange Commission (SEC) actions against Coinbase and others have made companies and their directors and officers consider the scope of their protection under insurance policies. Given the variety and volume of new crypto-related exposures, one question has been whether traditional property and casualty policies include coverage for crypto losses under insurance policies that arguably do not have explicit coverage for such losses.

This article addresses potential insurance coverage for crypto losses under various types of insurance policies and how to deal with insurers that reject crypto claims, as well as precautionary steps that companies and their executives can take to preempt, or alternatively to address, a denial of coverage.

Insurance Coverage for Crypto Losses

Companies may find potential coverage for their crypto-related losses under various lines of insurance, including under their directors and officers (D&O), errors and omissions (E&O), cyber, crime, and property policies. So far, companies and their executives have focused mainly on the potential for such coverage under D&O policies—especially when wrongdoing by management is alleged or a regulatory investigation is underway. D&O protects companies and their decision-makers when they are accused of

Robotics, Artificial Intelligence & Law / March–April 2024, Vol. 7, No. 2, pp. 133–139.

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

wrongdoing, as we have seen as a result of the recent collapses of crypto exchanges and adverse effects on companies with significant crypto-related exposure.

Exposures Are on the Rise, Even for Crypto-Adjacent Companies and Industries

The recent failures of companies in the crypto space and the sharp decline in the prices of cryptocurrencies have caused many companies to consider how to protect themselves in the volatile world of crypto. Several well-known crypto companies such as Genesis, Voyager Digital, Celsius, and BlockFi have reportedly filed for bankruptcy protection, reorganized, or gone out of business. While it is difficult to ascertain an exact number, losses are estimated to be substantial. Thus, companies and their executives have looked for ways to recoup crypto losses and hedge against similar risks and events in the future.

Basics of Private and Public D&O Coverage

D&O policies have, so far, been the central focus of potential coverage for crypto losses. Both private and public companies buy D&O coverage. D&O policies generally cover claims alleging wrongful acts against the company or its executives. The claims against the executives typically have to be for wrongful acts in their roles as directors or officers of the company. Insurers ordinarily define a wrongful act as any actual or alleged breach of duty, neglect, error or omission, misstatement, or misleading statement.

D&O policies issued to public companies normally cover the companies for securities claims for, among other things, alleged violations of laws related to the offer, solicitation, purchase, or sale of securities. D&O insurance for private companies, in contrast, typically includes coverage beyond that for securities claims, responding to any claim for "wrongful acts," a term that is defined broadly to include any act, error, omission, breach of duty, neglect, and other similar conduct. Thus, private companies can enjoy broader D&O insurance than publicly traded companies do because their coverage is not limited to securities claims, though

the individual executives should enjoy similar protection under D&O policies issued to both private and public companies. Still, the terms of each policy will ultimately dictate the scope of coverage for crypto losses, which is why the underwriting process is so important for policyholders.

Extent of Crypto Exposure and Insurance Underwriting Considerations

In procuring D&O and the other types of insurance identified above, companies should consider whether they are actively involved in transactions involving crypto currencies or doing business with other entities that have crypto exposure or who hold other types of digital assets such as non-fungible tokens (NFTs). A company's exposure to cryptocurrencies or NFTs can vary widely. For example, a company may hold one or multiple cryptocurrencies as assets on their balance sheets and may try to borrow against those assets. Another company may actively trade cryptocurrencies for its own account or broker such transactions for its customers. Perhaps the company has simply decided to accept crypto as a form of payment for its goods or services even if it immediately converts the crypto into fiat currency.

Regardless of the extent of the company's connection to crypto, the companies in the preceding examples would be exposed to a potentially covered crypto-related claim. Indeed, the company directly holding crypto may, for instance, have coverage for the loss in value of those assets while the company merely accepting crypto as a form of payment may be subject to shareholder lawsuits for management's decision to allow such payments. The potential claims against the company and its executives, and therefore the nature of subsequent insurance claims, can take many forms. The critical issue is for companies to evaluate their crypto exposure and try to account for that risk during the underwriting process for their insurance programs.

Although insurance policies can be amended during the coverage period, such amendments to expand coverage are not common, and the initial underwriting process is important because the policyholder company/insureds and prospective insurers typically define the scope of coverage at that time.

Exclusions and Other Potential Coverage Limitations

Many D&O policies can and should respond to claims involving crypto-related exposures. Negotiating favorable coverage terms during the underwriting process is only the first step toward maximizing potential D&O recoveries. The rubber really hits the road once a claim arises, as insurers may try to bar or limit coverage based on policy exclusions and other limiting language. Below are several D&O provisions that insurers could rely on to try to eliminate or reduce coverage for potential crypto-related claims that companies and executives should look out for.

Securities Claims

For public companies, one critical issue is whether shareholder crypto-related claims are "securities claims" and, more specifically, whether cryptocurrencies are "securities." Cryptocurrencies as "securities" could lead to an increase in regulatory scrutiny, but it also could mean more avenues for public company D&O coverage.

For example, the SEC pursued Ripple Labs Inc., a blockchain-based payments company, in a case over whether XRP, Ripple's digital currency, is an unregistered security. The SEC claimed that Ripple conducted a securities offering by selling XRP without proper registration. Ripple, however, maintained that XRP is a currency—not a security. Similarly, the SEC has sued Coinbase alleging it was operating its trading platform as an unregistered securities exchange, and is pursuing others on similar grounds. The litigation may have serious implications for the cryptocurrency industry because it could establish precedent for how crypto may be treated under U.S. securities laws. We expect future insurance coverage disputes over, among other things, the scope of coverage for securities claims involving cryptocurrencies or for government investigations involving cryptocurrencies.

Conduct Exclusions

D&O policies typically contain exclusions for claims against the company or its executives involving criminal or fraudulent acts. Insurers may try to invoke those exclusions to avoid coverage for regulatory or other government investigations alleging such wrongdoing against a company involved in crypto transactions.

Policyholders can reduce the effect of such an exclusion by, for example, insisting on language that the exclusion applies only upon a final, non-appealable adjudication that the company or its executives in fact are liable or guilty for those wrongful acts. If the exclusion is conditioned on a "final, non-appealable" adjudication, then, at a minimum, the company and its executives should have a right to advancement of defense costs until there is such an adjudication. However, in the event of an adverse final judgment that triggers the exclusion, the insurer may seek recoupment of the attorneys' fees and costs it incurred while defending the company or its executives. Thus, insureds may encounter a situation where they are facing not only an adverse ruling but also a claim from their D&O insurer for thousands or potentially millions of dollars in defense fees and costs. For that reason, among others, it is critical for policyholders to know whether the policy expressly allows for recoupment of defense fees and costs and, if so, under what terms, so policyholders can try to mitigate this risk. In addition, case law may preclude recoupment, and the Restatement of the Law, Liability Insurance does not support recoupment.

If insureds make claims for crypto losses or allegations, they should refuse to accept denials of coverage based on such exclusions, particularly where they require a "final adjudication" before they apply.

Bankruptcy and Insolvency

D&O policies may also contain insolvency exclusions, which can exclude coverage for claims or loss that arise out of or are sufficiently related to the insolvency of the insured company. Thus, if a crypto-related event threatens a company's solvency, its insurer may try to avoid coverage for the claim. Merely filing for bankruptcy does not necessarily eliminate a company's rights under its insurance policies. Cyber liability exclusions are becoming increasingly prevalent in D&O policies. Thus, those exclusions may also be implicated in some crypto-related claims. Indeed, as we have already seen, crypto exchanges have been targeted by cybercriminals who steal customer deposits. The executives of the hacked exchanges can face shareholder actions alleging, for example, that they breached their fiduciary duties allowing a cyberattack that resulted in the loss of cryptocurrency on deposit.

Similarly, insurers may try to use the professional services exclusions commonly found in D&O policies to try to avoid coverage for certain crypto-related claims. For example, an insurer may try to invoke the exclusion if the claim against the company or its executives is for rendering professional investment advice in the purchase or sale of cryptocurrencies or other digital assets. The D&O insurer may argue that such a claim is more appropriately covered under an E&O policy, which typically insure loss arising from the insured rendering or failing to render a professional service such as investment advice. The worst-case scenario for policyholders is an overly broad professional services D&O exclusion and a narrow definition of professional services in the coverage grant in an E&O policy. Such a dynamic could lead to the D&O and E&O insurers both refusing to provide coverage despite the policyholder having two policies intended to protect the company and its executives against those risks. This is an example of why it is critical for companies and their executives to have a holistic understanding of their insurance programs and where insurers may argue potential gaps in coverage may exist. Such arguments may be avoided by coordinating the coverage between the company's various policies.

As the preceding example showed, while D&O policies may not cover professional services rendered by the company or its employees, such coverage could be obtained through the purchase of E&O coverage. Thus, for proper risk management, a company should understand the coverage available under its suite of insurance policies, including the availability of extended reporting periods and tail coverages that may apply under certain circumstances; for example, following an acquisition or bankruptcy.

Conclusion

Cryptocurrencies, their value, and social utility (or lack thereof) can be polarizing topics. Personal views aside, in the execution of obligations to the company, executives should carefully assess any potential crypto-related exposures and whether and to what extent those exposures are addressed by the company's insurance program. Companies should seek to understand how they will respond to recalcitrant insurers that refuse to cover crypto claims, and take precautionary steps to preempt a denial of coverage based

on the exclusions discussed above. Indeed, a policyholder facing a claim denial based on an exclusion should remind the insurer of its burden of establishing that the exclusion applies to eliminate coverage for the crypto-related claim.

Beyond that, to enhance the predictability of how the insurer will try to use the exclusions or other limiting language in the policy, policyholders can influence its construction by negotiating the precise language with the insurer. This approach will also help document exactly what type of loss the parties intended to insure.

Note

* The authors, attorneys with Hunton Andrews Kurth LLP, may be contacted at mlevine@huntonak.com, gfehling@huntonak.com, lmasters@huntonak.com, and yabreu@huntonak.com, respectively.