Proskauer

Beyond the Screen: Clickwrap Principles Reach Crypto Kiosks

New Media and Technology Law Blog on **March 18, 2026**

A recent decision from an Indiana federal court underscores that the principles behind what makes "clickwrap" assent enforceable are not limited to websites and apps found through smartphones and laptops. In *Beckett v. Bitcoin Depot, Inc.*, No. 25-01450 (S.D. Ind. Feb. 26, 2026), the court granted a Bitcoin ATM operator's motion to compel arbitration, finding that the plaintiff—who had fallen victim to a cryptocurrency scam—assented to the company's clickwrap terms before completing the transactions.

The ruling is notable because most electronic "clickwrap" contracting cases focus on the issues involving websites or mobile apps. While there was no reason to expect a different analysis in the context of a kiosk, *Beckett* clarifies that those familiar principles extend into the physical world of kiosk screens and self-service terminals.

The takeaways are clear:

- First, contracting rigor matters just as much in kiosk environments as it does online. Providers should implement thoughtfully designed user flows that mirror best practices from ecommerce: clear and uncluttered interfaces, conspicuous presentation of terms, affirmative assent mechanisms, and reliable audit logs.
- Second, and specific to the fact that this was a crypto case, robust anti-fraud warnings can serve a dual purpose. Beyond helping protect consumers, they may also strengthen litigation defenses, particularly on issues of notice, assumption of risk and causation.

The Facts

Bitcoin ATMs (or "BTMs") are kiosks that allow users to purchase—and sometimes sell—cryptocurrency. Rather than dispensing cash, they typically accept cash or debit card payments and transfer cryptocurrency to a wallet specified by the user, often via QR code.

The plaintiff, a retiree, was targeted in a “tech support” impersonation scam. He was persuaded to withdraw cash from his bank accounts on three separate occasions and use a BTM operated by Bitcoin Depot to transfer funds to a third-party digital wallet controlled by the scammers. This type of scam is common and was the subject of a September 2024 Federal Trade Commission (FTC) consumer alert.

In the end, the funds could not be recovered, and the plaintiff brought suit asserting tort and consumer protection claims and alleging that Bitcoin Depot failed to implement adequate safeguards.

The Contracting Flow

Before completing each transaction, the plaintiff was required to accept Bitcoin Depot’s terms and conditions on-screen. The process included multiple layers of warning and verification:

- A prominent red-text warning cautioned: *“If someone else sent you to this machine and provided you with a QR Code or wallet ID to send funds to, it is most likely a scam.”*
- A follow-up text message warned against sending funds to purported government officials, law enforcement or tech support, and against using third-party QR codes.
- The user was required to enter a PIN sent via text message.
- The interface then presented a direct prompt: *“ARE YOU BEING SCAMMED?”* along with examples of common fraud scenarios and advising users that losses due to fraudulent transactions may not be recoverable.
- Finally, the user had to confirm that the destination wallet belonged to them; selecting any other option would cancel the transaction.

Despite these warnings, the plaintiff confirmed—incorrectly—that the destination wallet was his own.

The Court’s Ruling

Bitcoin Depot moved to compel arbitration under its terms of service. The court granted the motion, emphasizing that the plaintiff did not dispute that he had assented to the arbitration agreement on three separate occasions. Arguments regarding unconscionability and other enforceability issues were left for the arbitrator to decide.

Final Thoughts

This case reinforces a straightforward but important point: enforceable digital contracting principles apply wherever transactions occur, including at physical kiosks.

At the same time, the case hints at future litigation risk. While Bitcoin Depot secured a procedural win, different facts could lead to closer scrutiny of a provider's safeguards. Plaintiffs may increasingly attempt to move beyond contract formation and challenge the reasonableness and adequacy of provider's risk controls and safety messaging. For example, the complaint in *Beckett* outlines several allegedly "inadequate safeguards," such as claims that Bitcoin Depot failed to implement transaction limits for first time elderly users, monitor large sequential deposits, or flag certain scenarios like repeated maximum value deposits to the same digital wallet.

Related Professionals

- **Jeffrey D. Neuburger**