Proskauer

Consumer Law Claims against French Crypto Asset Wallet Provider May Proceed in California Court

Blockchain and the Law on **January 18, 2023**

Customer lists held by providers and the personal information users enter to obtain digital wallets or set up crypto exchange accounts are enviable targets for hackers. Such data can be used to launch targeted phishing schemes and related scams to trick holders into divulging their private keys or else unknowingly transferring anonymized crypto assets to hackers. One recent case involves a suit brought by customers who purchased a hardware wallet to secure cryptocurrency assets and are seeking redress for harms they allegedly suffered following data breaches that exposed their personal information.

A recent Ninth Circuit decision analyzed whether a federal court had personal jurisdiction over a foreign crypto asset wallet provider, an issue that can be important when litigating in this area, given the boundary-less nature of the world of crypto assets and related services. (*Baton v. Ledger SAS*, No. 21-17036 (9th Cir. Dec. 1, 2022) (unpublished)).

In the case, plaintiffs bought hardware wallets to store crypto assets. Following data breaches which allegedly exposed personal information provided in relation to the wallet purchases (e.g., names, email addresses, postal addresses and telephone numbers), plaintiffs brought suit against Ledger SAS ("Ledger"), the French company that produced and sold the wallets and Shopify Inc., ("Shopify") the Canadian company that provided e-commerce services for Ledger's store, and its U.S. subsidiary (collectively, "Defendants"). Plaintiffs brought various claims in California district court, including negligence and California and other state consumer claims based on their allegation that Ledger failed to exercise reasonable care in securing their personal information.

In moving to dismiss, defendants claimed the court lacked personal jurisdiction over them: Shopify Inc. argued that it is a Canadian corporation that is not registered to do business in California and does not have any employees in California and that the "rogue" individuals who were responsible for one data breach of Shopify, Inc.'s platform (including, purportedly, some Ledger customer transactional records) were not employees of Shopify, but foreign contractors; Ledger contended that it is a French company with no California or U.S. employees. The district court granted the motions and dismissed the action for lack of personal jurisdiction over the defendants. The lower court found no specific jurisdiction over Shopify simply because it provided a software product that allowed Ledger to run an online store to consumers worldwide, as it was Ledger, not Shopify, which made a conscious choice to purposefully direct its product toward the California forum. Second, the court denied, as "speculative" and "unwarranted" plaintiffs' request for jurisdictional discovery seeking information about, among other things, the existence of employees who may have worked with the "rogue" contractors involved in one breach and the alleged activities of a particular California-based data protection officer at Shopify. As to defendant Ledger, the lower court similarly found that merely operating a universally accessible website alone is generally insufficient to satisfy the requirement that Ledger "expressly aimed" its conduct to California.

The Ninth Circuit reversed the dismissal of the action, affirming in part, and reversing in part, the lower court's findings on jurisdiction. (*Baton v. Ledger SAS*, No. 21-17036 (9th Cir. Dec. 1, 2022) (unpublished)). The appeals court found the court had personal jurisdiction over Ledger because of its sales in the state, totaling about 70,000 wallets sold to Californians, generating millions of dollars in revenue. The court also stated that Ledger's website is designed to collect the applicable California sales tax for buyers whose IP addresses are in California. Taken together, such facts establish "purposeful availment" because Ledger's contacts with the forum cannot be characterized as "random, isolated, or fortuitous." The court also stated that plaintiffs' claims "arise out of" those wallet sales since the personal information was collected for e-commerce and marketing purposes. Still, the court limited the potential universe of claims that plaintiffs' putative class could bring based upon the existence of a broad forum selection clause in Ledger's terms that mandates "[a]ny dispute, controversy, difference or claim arising out of or relating to" the terms be brought exclusively in French courts. The court held that the forum selection clause was enforceable, except with respect to claims under California consumer laws brought by California residents, finding such claims could not be waived based on public policy grounds.

As to Shopify, the Ninth Circuit agreed that the present record does not support personal jurisdiction, but held that the lower court wrongly refused plaintiffs' requests for jurisdictional discovery and an opportunity to amend the complaint following such discovery. The court noted that Shopify USA employs a number of people who work remotely from California, and that apparently one of those employees, at the relevant time, had the title of "Vice President, Legal; Data Protection Officer." In the appeals court's view, it is reasonable to infer that Shopify's Data Protection Officer in California "may have played a role related to the data breach because he appears to have overseen the relevant privacy policies and Shopify's response," but that more facts were needed to determine whether such activities supported the exercise of jurisdiction.

2022 saw a record increase in the number of crypto-related hacking incidents (one report found over $3 billion in stolen cryptocurrency from January through October). Security incidents have particularly affected decentralized protocols, including cross-chain bridges and the smart contracts underlying DeFi, some of which may have been built on imperfect code. These hacking incidents are occurring during the enduring crypto winter downturn, which has been exacerbated by recent high profile collapses and bankruptcies in the industry. One would expect more litigation brought by users against providers over crypto assets stolen by hackers.

Moreover, this case signals that crypto-related businesses outside the United States may be subject to jurisdiction within the country, notwithstanding limited contacts within its borders. Given the size of the U.S. market, this may be a risk worth taking. To minimize the risk, depending on the particular business, there may be steps that can be taken to reduce the likelihood of such a finding.

View original.