ALSTON & BIRD

PAYMENTS DOCKET

- NEW LAWSUITS FILED
- PENDING MOTIONS

ISSUE ONE | JUNE 2022

NEW LAWSUITS

New Class Actions Allege That Payments Network Has Not Protected Users from Fraud

Stock v. Wells Fargo & Co, et al., No. 8:22-cv-00763 (C.D. Cal.).

Arant v. Early Warning Services LLC, No. CV2022-005057 (Sup. C. Maricopa Cnty., Ariz.).

Wilkins v. Navy Federal Credit Union, No. 2:22-cv-02916 (D.N.J.).

Over the past few months, there has been a spate of putative class actions accusing banks and related companies of not doing enough to protect their customers from scams aimed at users of Zelle. So far, these suits have been filed in California, Arizona, and New Jersey and allege violations of the federal Electronic Fund Transfer Act and various state consumer protection statutes.

In the *Stock* case, for example, the plaintiff alleges that she was tricked by a caller impersonating a Wells Fargo customer representative into signing up for Zelle, and then sharing a Zelle verification code that had been sent to her via text. The plaintiff alleges that the scammer used the verification code to steal $1,000 from her Wells Fargo account and that the bank refused to credit the plaintiff's account after investigating the transaction.

The *Stock* complaint asserts claims under the Electronic Fund Transfer Act, violations of California's Unfair Competition Law, and negligence. The plaintiff seeks to represent a nationwide class of individuals whose accounts were debited via Zelle and not fully credited within 45 days of disputing the transaction with their bank. The complaint also seeks certification of a similarly defined California subclass.

Another case has been filed in Arizona making similar allegations against Early Warning Services LLC, the entity that owns and operates Zelle. There, the plaintiff seeks to certify a class of all Zelle users who incurred unreimbursed losses to due to fraud and further seeks to certify a Washington State subclass. The complaint asserts claims for alleged violations of Arizona's Consumer Fraud Act and Washington's Consumer Protection Act.

More recently, plaintiffs targeted Navy Federal Credit Union with a similar suit in New Jersey. There, the named plaintiff alleges that she was tricked into making a payment via Zelle to what she thought was her electric utility, but in fact was a fraudster impersonating the utility. The plaintiff alleges that Navy Federal failed to disclose the risks of using Zelle, which allegedly include that funds transferred by mistake or due to fraud are essentially unrecoverable.

Retailer Seeks to Recover $10.7 Million in Penalties Arising from Data Breach

Wawa Inc. v. Mastercard International Inc., No. 7:22-cv-03186 (S.D.N.Y.).

Wawa has sued Mastercard to recover an allegedly unlawful $10.7 million penalty it paid after a data security incident that Mastercard says was caused by Wawa's violation of the Payment Card Industry Data Security Standard (PCI DSS).

The case arose after Wawa discovered a data security incident in 2019 that resulted in unauthorized access to its cardholder data environment. Wawa notified its payment processor of the data incident. The processor, in turn, had contractual obligations to notify Mastercard of the potential exposure of its cardholders' data. The processor's contract with Mastercard also exposed it to potential liability for merchants' noncompliance with various card network rules, including the PCI DSS.

Wawa asserts that, after an investigation, Mastercard decided to impose an over $17 million assessment on Wawa's processor because of the data breach. Though the processor appealed, and Mastercard exercised its discretion to reduce the assessment to approximately $10.7 million, the processor nevertheless sought indemnification and reimbursement from Wawa per the parties' payment processing contract. Wawa agreed to pay the full amount of Mastercard's assessment on its processor and, in exchange, the processor assigned Wawa its rights and claims against Mastercard related to the assessment. That assignment is what allowed Wawa to file suit against Mastercard.

Wawa, as assignee, claims that Mastercard breached its contract with Wawa's processor because Mastercard incorrectly determined that the security incident violated Mastercard's standards and that violations of the PCI DSS caused the incident. Wawa further claims that Mastercard's assessment was not based on losses actually incurred by Mastercard as a result of the incident; therefore, the assessment was a violation of the implied duty of good faith and fair dealing. Finally, Wawa asserts claims, both directly and as assignee for its processor, for unjust enrichment and for violations of New York's and North Carolina's deceptive trade practices statutes.

Plaintiff Files Amended Complaint Against Cellular Provider After Alleged Theft of Cryptocurrency

Li, et al. v. AT&T Mobility LLC, No. 5:22-cv-00431 (C.D. Cal.).

Amwear USA and its employee, Scott Li, using a novel theory in the rapidly evolving cryptocurrency universe, have filed an amended complaint against AT&T Mobility LLC after the employee's corporate cellular phone number was used in connection with the alleged theft of approximately half a million dollars in cryptocurrency. The plaintiffs allege that AT&T transferred the employee's phone number to another cellular service provider without the employee's authorization, in violation of the underlying cellular service contract. According to the plaintiffs, the phone number was then used to pilfer approximately $500,000 of cryptocurrency from unnamed software applications. The plaintiffs originally asserted claims for breach of contract and breach of the duty of good faith and fair dealing. They also sought to recover the value of the allegedly stolen cryptocurrency, plus interest, attorneys' fees, and costs.

AT&T filed a motion to dismiss the complaint under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim, which the trial court granted on April 21, 2022. Notably, the trial court held that the employer could not state an express or implied breach of contract claim because it did not suffer any damages; rather, the allegedly stolen cryptocurrency belonged to the employee. The court also held that the complaint failed to adequately allege causation because "nothing in the complaint explains how Plaintiff Li's temporary loss of 'access' to Defendant's cellular service could have resulted in $500,000 worth of cryptocurrency being removed from an account maintained by a completely separate company."

Following dismissal, the plaintiffs filed an amended complaint restating the two prior breach claims and adding four new causes of action, including a statutory unauthorized disclosure claim under the federal Communications Act, two California statutory claims—one for unauthorized computer access under the California Penal Code and the other under the California Customer Records Act—and a claim seeking a declaration that the underlying contract is unenforceable under California law. AT&T again moved to dismiss the amended complaint for failure to state a claim for relief, which currently remains pending before the trial court.

A New Wave of Class Actions Challenges Bank "Buy Now, Pay Later" Payments Plans

Michael Sliwa v. Sezzle Inc., No. 2:22-cv-03055 (C.D. Cal.).

"Buy now pay later" (BNPL) programs—which give retail consumers the option to spread payments over several installments, usually on an interest-free basis—are experiencing rapid growth. As those programs have grown, they have attracted the attention of plaintiffs' law firms. Within the last two months alone, several putative class actions have been filed across the country against providers of BNPL programs. The gist of these lawsuits is that BNPL providers violate state consumer protection statutes by falsely representing the programs as interest free, when in fact BNPL users are potentially liable for bank overdraft fees when customer accounts have insufficient funds to cover BNPL installment payments. All of the suits allege that BNPL companies target low-income consumers who are allegedly most vulnerable to overdraft fees and related bank charges.

One example is a suit brought in late May 2022 against Sezzle, which operates a BNPL service. The plaintiff alleges that he incurred overdraft fees when Sezzle attempted to draw an installment payment from his account and there were insufficient funds to cover it. The plaintiff claims that Sezzle markets its service as allowing purchasers to buy now, pay later with "no interest," but fails to warn users of the risk that they may become liable for insufficient funds fees or overdraft fees. The plaintiff also alleges that Sezzle knows that its BNPL service specifically targets low-income consumers who are more likely to incur large bank fees if they are unable to timely pay the installments. The complaint asserts claims for violations of California's Unfair Competition Law, California's False Advertising Law, and Minnesota's Consumer Fraud Act.

PENDING MOTIONS

Payment Processor Seeks to Duck Merchant Class Action Alleging Excessive and Hidden Processing Fees

Braids R Us 305, et al. v. Priority Payment Systems LLC, et al., No. 1:21-cv-05318 (N.D. Ga.). *Paul Judith Enterprises Inc., et al. v. Priority Payment Systems LLC, et al.*, No. 1:22-cv-01305 (N.D. Ga.).

In a filing in the Northern District of Georgia, payment processor Priority Payment Systems LLC asked the court to toss nearly all claims brought by a group of plaintiffs seeking to represent two nationwide classes of merchants that were allegedly charged excessive or hidden processing fees. Priority argued that the class action "is pled with the formulaic hyperbole that has become the tired signature of putative merchant class actions" and therefore fails to state a claim under Federal Rule of Civil Procedure 12(b)(6). Specifically, Priority argued that the plaintiffs' fraud and breach of contract claims are doomed by the express terms of the parties' contract, which allegedly permitted Priority to undertake the very actions underlying the putative class members' claims. Priority also argued that the parties' contract defeats the plaintiffs' unjust enrichment claims as a matter of settled Georgia law and that the payment processor could not have violated the implied covenant of good faith and fair dealing by doing precisely what the contract permitted it to do.

While Priority's motion to dismiss was pending, the parties consented to consolidate a second—and nearly identical—case, *Paul Judith Enterprises*, into the *Braids R Us* litigation. If the court approves the consolidation, then the *Paul Judith Enterprises* litigation would be tolled pending resolution of the pending motion to dismiss.

Technology Startup to Pay $58 Million to Settle Claims of Nearly 100 Million Putative Class Members

In re Plaid Inc. Privacy Litigation, No. 4:20-cv-3056 (N.D. Cal.).

Plaid Inc.—a technology startup providing bank "linking" and verification services for FinTech apps that consumers use to send and receive money from their financial accounts, such as Venmo, Coinbase, Cash App, and Stripe—sought final approval of its plan to settle the claims of nearly 100 million putative class members for a lump-sum payment of $58 million.

In the underlying case, the plaintiffs alleged that Plaid deceived consumers into providing their bank account credentials by causing them to believe that they were entering their credentials on the financial institutions' log-in pages when, in reality, they were providing that information directly to Plaid. Plaid is alleged to have then stored, analyzed, and sold "a staggering amount of consumer banking data." Plaid sought dismissal on various standing- and claims-based grounds, which the court granted in part and denied in part. The surviving claims were for invasion of privacy/intrusion into private affairs and unjust enrichment, as well as a California-only class asserting California-specific constitutional and statutory claims. The parties' settlement discussions escalated shortly thereafter, ultimately culminating in this settlement agreement.

Under the terms of the settlement, the class members will share the settlement funds on a pro rata basis. Plaid will also be required to maintain certain changes to the design of its standard interface, make more fulsome disclosures to consumers, and delete transactional banking data for consumers whose apps did not request that data. The parties' motion for final approval of the settlement is pending before the trial court.

Contributing Authors

David E. Meadows
Partner
404.881.7963
david.meadows@alston.com

Alexandra S. Peurach
Partner
404.881.7974
alex.peurach@alston.com

Kaylan Meaza
Senior Associate
404.881.7412
kaylan.meaza@alston.com

Christopher Kelleher
Associate
404.881.7435
chris.kelleher@alston.com

Additional Payments Litigation Professionals

Michael Agoglia
Partner
415.243.1011
michael.agoglia@alston.com

Christopher Riley
Partner
404.881.4790
chris.riley@alston.com

Kelley Connolly Barnaby
Partner
202.239.3687
kelley.barnaby@alston.com

Elizabeth Sperling
Partner
213.576.1028
e lizabeth.sperling@alston.com

Learn more about our Payments Litigation team

ALSTON & BIRD