The Continued Erosion Of Overbroad Class Actions - The Ninth Circuit Takes Action

Scott O'Connell
Nicon Peabody (Boston, MA)

soconnell@nixonpeabody.com | 617.345.1150
http://www.nixonpeabody.com/scott_oconnell

The Supreme Court's pro arbitration message from Concepcion has once again reached the Ninth Circuit U.S. Court of Appeals with a direct impact on California's Unfair Competition Law. In its March 7, 2012, decision in the putative class action captioned *Kilgore, et al. v. KeyBank, National Association*, No. 09-16703, a three-judge panel of the Ninth Circuit[1] scuttled a line of California cases[2] mandating that arbitration agreements in California are not enforced where the plaintiff is "functioning as a private attorney general" in that the only relief sought is an injunction "enjoining future deceptive practices on behalf of the general public." *Id.* at 2645 (quoting *Broughton v. Cigna Health-plans of California*, 988 P.2d 67, 76 (Cal. 1999)). Despite misgivings that the ruling might reduce the effectiveness of California's robust consumer protection laws, the Ninth Circuit concluded that, following the Supreme Court's recent decision in *AT&T Mobility LLC v. Concepcion*, 131 S. Ct. 1740 (2011), there could be no doubt that the Federal Arbitration Act ("FAA") preempts the California law. The Ninth Circuit also ruled that the plaintiffs could not prevail on their alternative argument that the arbitration clause was unconscionable because KeyBank provided its borrowers with a meaningful opportunity to "opt-out" of arbitration.

The *Kilgore* lawsuit was brought by two disgruntled students of Silver State Helicopters, LLC ("SSH"), a national aviation school that closed operations and declared bankruptcy in February 2008. KeyBank had been one of the lenders to SSH students. The plaintiffs, seeking to represent a class of former California-based SSH students, claimed that SSH did not deliver on the education it promised, and that under California's Unfair Competition Law ("UCL"), KeyBank, as a preferred lender, should be held liable for SSH's failures. Seeking a judicial forum for their class action, the plaintiffs filed four different complaints, the last one of which contained carefully crafted allegations to trigger California's public injunction exception. Rather than seeking damages from KeyBank, the plaintiffs asked for an order enjoining KeyBank from enforcing its SSH promissory notes and from reporting delinquencies to the credit reporting agencies. Each of those promissory notes contained an arbitration clause providing that either party could elect binding arbitration of any disputes.

KeyBank elected to arbitrate the dispute and filed a motion asking the U.S. District Court for the Northern District of California to stay the Kilgore lawsuit and compel arbitration. Judge Thelton E. Henderson denied KeyBank's motion based on California's policy against arbitrating cases seeking a public injunction. KeyBank preserved the arbitration issue by immediately filing for interlocutory appeal pursuant to the FAA, but the district court retained jurisdiction and ruled on KeyBank's alternative motion to dismiss.[3] Ironically, the district court granted KeyBank's motion to dismiss, ruling that the National Bank Act and the regulations of the Office of the Comptroller of the Currency preempt plaintiffs' UCL claims. Plaintiffs appealed the district court's dismissal order to the Ninth Circuit and that appeal was consolidated with KeyBank's appeal of the arbitration decision.

The Ninth Circuit panel viewed the arbitration appeal as a threshold issue. Analyzing the text of the FAA, the panel recognized that where the parties to a contract have agreed to arbitration, the FAA "leaves no place for the exercise of discretion by a district court, but instead mandates that district courts shall direct the parties to proceed to arbitration." *Id.* at 2640 (quoting *Dean Witter Reynolds, Inc. v. Byrd*, 470 U.S. 213, 218 (1985)). The limited exception to this mandate is where the arbitration clause would be unenforceable "upon such grounds as exist at law or in equity for the revocation of any contract." *Id.* at 2641 (emphasis added) (quoting 9 U.S.C. § 2). Thus, "a state statute or judicial rule that applies only to arbitration agreements, and not to contracts generally, is preempted by the FAA." *Id.*

As the Ninth Circuit acknowledged, the recent ruling in *Concepcion* is just the latest in a line of Supreme Court cases that have vigorously applied FAA preemption against state laws that are hostile to arbitration. In *Concepcion*, the Supreme Court threw out California's *Discover Bank* rule, which had prohibited as unconscionable all arbitration clauses that require a consumer to arbitrate all disputes in an individual bilateral arbitration and never as part of a plaintiff or class member in a class action proceeding.[4] The Court ruled that the FAA preempted California's anti-class action waiver rule because "[r]equiring the availability of classwide arbitration interferes with fundamental attributes of arbitration and thus creates a scheme inconsistent with the FAA." *Id.* at 2644 (quoting *Concepcion*, 131 S. Ct. at 1748). Notably, the Court stated that states "cannot require a procedure that is inconsistent with the FAA, even if it is desirable for unrelated reasons." Id. (quoting *Concepcion*, 131 S. Ct. at 1753).

The Ninth Circuit recognized that the rationale of *Concepcion* also mandates the end of California's public injunction rule. That rule prohibits arbitration of claims that seek an injunction for the benefit of the public. Because the California rule "prohibits outright the arbitration of a particular type of claim, the analysis is straightforward: The conflicting rule is displaced by the FAA." *Id.* at 2643 (quoting *Concepcion*, 131 S. Ct. at 1747); *see also Id.* at 2650 (citing In *Marmet Health Care Center, Inc. v. Brown*, Nos. 11-391 and 11-394, 2012 U.S. LEXIS 1076 (Feb. 21, 2012) (per curiam) (preempting West Virginia law that prohibited arbitration of personal injury and wrongful death claims). In other words, Congresses' judgment, embodied in the text of the FAA, that all valid agreements to arbitrate should be enforced trumps any state legislature's conclusion that arbitration is not suitable in some cases.

The Ninth Circuit recognized, however, that *Concepcion* did not overthrow general common law contract defenses like unconscionability. The Court ruled that KeyBank's arbitration clause was not procedurally unconscionable because it was conspicuously displayed in the promissory note and was written in plain language. *Id.* at 2655. More importantly, the promissory note provided a meaningful opportunity for the borrower to opt-out of the arbitration agreement by submitting an opt-out notice to KeyBank in writing within 60 days. The promissory note set forth in plain language, in multiple locations in the document, the rights that plaintiff would waive by failing to opt-out. *Id.* The panel rejected plaintiffs' arguments that KeyBank did not go far enough. The opt-out instructions were clear and easy to follow, and, even to the extent that "Plaintiffs claim that they were so 'intoxicated by helicopters' that they never saw the arbitration clause, [the Court] refer[s] them to the end of the Note. Immediately above each Plaintiff's signature line is a warning that the student should read the contract carefully before signing, as well as a promise from the student that he would do so 'even if otherwise advised.'" *Id.* at 2656. Finding that the arbitration clause was not procedurally unconscionable, the Court did not address whether the terms of the clause were substantively unconscionable. *Id.*

Having concluded that the motion to compel arbitration should have been granted, the Ninth Circuit found that the district court's dismissal order was a nullity. The Ninth Circuit vacated the judgment in favor of KeyBank and remanded to the district court with instructions to enter an order staying the case and compelling arbitration. Thus, by winning its arbitration argument, KeyBank's favorable judgment on the merits based also on preemption was vacated. But given the broad repercussions of this ruling, including the expansion of *Concepcion* and the Ninth Circuit's explicit validation of KeyBank's arbitration clause and opt-out provision, it was a worthwhile exchange. Additionally, while the two *Kilgore* plaintiffs may continue to pursue their claims, they must do so as individuals as the arbitration agreement has a class waiver.

For consumer-facing companies with arbitration agreements, the *Kilgore* opinion is an important read to assess whether your provision would pass the unconscionability filter applied by this Court. Also, if you are managing cases in which efforts to compel arbitration have been defeated because injunctive relief is involved, this authority gives new vitality to your argument.

Nixon Peabody was counsel to KeyBank in this proceeding.

[1] Circuit Judges Stephen S. Trott and Carlos T. Bea, and District Judge Rebecca R. Pallmeyer, sitting by designation.

[2] *Broughton v. Cigna Health-plans of California*, 988 P.2d 67 (Cal. 1999); *Cruz v. Pacificare Health Systems, Inc.*, 66 P.3d 1157 (Cal. 2003). See also *Davis v. O'Melveny & Myers*, 485 F.3d 1066, 1082 (9th Cir. 2007) (applying California rule against arbitrating actions seeking public injunctions).

[3] Unlike the majority of other circuits, in the Ninth Circuit the district court is not divested of jurisdiction upon a timely filed interlocutory appeal. That situation resulted in further proceedings before the district court while the appeal was pending.

[4] *Discover Bank v. Superior Court,* 113 P.3d 1100 (Cal. 2005).

First Circuit faults bank for "one-size-fits-all" approach to cyber security measures

by W. Daniel Deane, Scott O'Connell

Following a landmark decision in July by the First Circuit U.S. Court of Appeals in Boston, commercial banks are advised to review their cyber security measures. The First Circuit's ruling, that the cyber security measures employed by a local community bank in Maine were not "commercially reasonable," resuscitates a business customer's attempt to hold its bank liable for six unauthorized transfers totaling nearly $350,000. The decision, Patco Construction Co. v. People's United Bank[1], authored by Chief Judge Sandra Lynch, hinges on interpretation of Article 4A of the Uniform Commercial Code ("UCC"),[2] which allocates the risk of loss between parties involved in "funds transfers."[3] As the First Circuit is the first federal appellate court to interpret the meaning of "commercially reasonable" in the context of an Article 4A claim, the ruling is likely to have a broad impact in the industry.

The plaintiff, Patco, is a small property developer and contractor located in southern Maine that began banking with Ocean Bank,[4] a local community bank, in 1985. Patco enrolled in Ocean Bank's "eBanking" program in 2003, primarily for making weekly payroll payments. Ocean Bank took steps to ensure the safety and security of its online banking platform, including purchasing the Jack Henry & Associate's "Premium" security package, which employed six key features: (1) user IDs and passwords; (2) invisible device authentication (i.e., placing a "cookie" onto customers' computers so that they could be identified in the future); (3) an adaptive risk profiling and monitoring system; (4) the use of "challenge questions" for specified situations; (5) a dollar amount rule that would result in an alert or other procedure for every transfer made above a threshold amount; and (6) a subscription to the eFraud Network, which maintains a database on known frauds.

Despite these safeguards, in May 2009, hackers somehow acquired Patco's user IDs, passwords, and "challenge question" answers, and transferred $588,851 from Patco's account into unauthorized third-party accounts. Ocean Bank quickly blocked or recovered some of the money, but Patco was left with a residual loss of $345,444. The parties disagree as to how Patco's authentication credentials were stolen. Patco claims that hackers employed a "keylogger," a form of computer malware that imbeds itself within the victim's computer system and records the user's keystrokes when the user logs onto a financial website. That keystroke information is then transmitted to the hacker. Ocean Bank, however, theorizes that Patco's credentials may have been compromised by the negligence of its employees.

In September of 2009, Patco sued Ocean Bank, then a division of People's United, in a six-count complaint asserting liability under Article 4A of the UCC, and several common law theories of liability including negligence, breach of contract, breach of fiduciary duty, and unjust enrichment. Less than a year into the case, the federal district court in Maine granted summary judgment in favor of the defendant bank, ruling that it was not liable under Article 4A because it had employed "commercially reasonable" security measures, and that the remaining counts were either preempted by the UCC provision or could not succeed for the same reasons. Construing the meaning of "commercially reasonable" for Article 4A purposes, and writing on a blank slate, the First Circuit reversed the grant of summary judgment and remanded the case back to the district court for further proceedings.

The First Circuit began its analysis by noting the risk-shifting scheme created by Article 4A. Under that scheme, the bank receiving the payment order initially bears the risk of loss for any unauthorized transfer. That risk of loss can be shifted to the customer if the bank can establish an agency relationship between the sender of the order and the customer. Commentary to Article 4A recognizes, however, that establishing an agency relationship is difficult in the electronic age, where payment and transfers are ordered by a message on a computer screen. Accordingly, the drafters of Article 4A provided a second method for shifting the risk of loss.

Where the bank and its customer have agreed to electronic transfers verified by a security procedure, an electronic transfer is effective, even if unauthorized, if: (a) the security procedure "is a commercially reasonable method of providing security against unauthorized payment orders," and (b) the "bank proves that it accepted the payment order in good faith and in compliance with the security procedure and of any written agreement or instruction of the customer." Patco, 2012 U.S. App. LEXIS 13617, at *29-30 (quoting Me. Rev. Stat. Ann., tit. 11, § 4-1202(2)). Critically, the commercial reasonableness of a security procedure depends on the needs and circumstances of each particular customer. Article 4A provides that banks should consider "the wishes of the customer" as well as "the circumstances of the customer," including the "size, type and frequency of payment orders normally issued by the customer to the bank"; alternative available security procedures; and security procedures "in general use by other customers and receiving banks similarly situated." Id. at *30-31 (quoting Me. Rev. Stat. Ann., tit. 11, § 4-1202(3)).

The First Circuit found that Ocean Bank's security procedures failed the Article 4A test because they were employed in a "one-size-fits-all" manner, rather than being tailored to the particular needs and circumstances of Patco. Id. at *41. In particular, although Ocean Bank had purchased Jack Henry's "Premium" security package, there were two critical flaws in how Ocean Bank used the system. First, Ocean Bank did not tailor its dollar amount indicator to Patco's circumstances. Initially, Ocean Bank set the dollar amount indicator at $100,000. For any transfer of $100,000 or more, the user was required to answer the "challenge questions" that had been created by the customer. In June 2008, Ocean Bank lowered the dollar amount threshold to $1. But all of Patco's payroll withdrawals were in the tens of thousands and never exceeded $37,000. Accordingly, before June 2008, none of Patco's transfers would have triggered the dollar amount threshold, and after June 2008, every Patco transfer triggered it. Because Patco was effectively required to answer the challenge questions for every weekly payroll transfer after June 2008, the risk of a keylogger attack was greatly increased. If Patco's computer systems were attacked by a keylogger, it was more likely that the keylogger software would record the challenge question answers (along with the user ID and password) before the customer could detect and remove the malware. Thus, Ocean Bank's overuse of challenge questions actually increased the risk of cyberattack.

Second, Ocean Bank did not take full advantage of Jack Henry's adaptive risk profiling and monitoring system. The Jack Henry system monitored Patco's transactions and generated risk-scoring reports based on criteria designed to detect suspicious activity. The May 2009 unauthorized transfers were scored as "high risk" because they did not match the predictable profile of an authorized Patco transfer. Patco payments were generally processed weekly on Fridays, never exceeded $37,000, were ordinarily directed to the same accounts, and always originated from a single static IP address located at Patco's offices in Sanford, Maine. The monitoring system did not work, however, because Ocean Bank personnel did not review these risk-scoring reports. The only consequence of a high risk score was that the user attempting to process the transaction would be prompted to answer the challenge questions, which the customer would be required to do for all transactions after June 2008 in any event. Thus, by lowering the dollar amount threshold to $1 and by failing to monitor the risk-scoring reports, Ocean Bank failed to reasonably account for Patco's particular circumstances. According to the First Circuit, Ocean Bank's procedures effectively "deprived the complex Jack Henry risk-scoring system of its core functionality." Id. at *37.

The First Circuit also criticized Ocean Bank for failing to take advantage of any additional emerging security technologies. See id. at *41-42. For example, Patco's expert testified that by May 2009, many other commercial banks employed hardware-based tokens, which generate one-time passwords that are constantly refreshed within seconds. Banks that do not use tokens use some other form of additional security, such as manual review of transactions or customer verification with regard to suspicious activity. In light of the flaws in Ocean Bank's security procedure, and its failure to implement additional and more reliable methods, the First Circuit concluded that Ocean Bank's security procedure was not commercially reasonable. The First Circuit also disagreed with the district court that the breach of contract and breach of fiduciary duty claims were preempted by Article 4A, and it therefore revived those claims, too.

Perhaps the silver lining for banks is the First Circuit's recognition that Article 4A is not "a one-way street," as it imposes obligations and responsibilities on customers as well as banks. Id. at *47. Acknowledging that legal and factual issues remained with regard to Patco's claims, the First Circuit affirmed the district court's denial of Patco's cross-motion for summary judgment. The First Circuit remanded the case to the district court for consideration as to whether, and if so, to what extent, the customer still bears any obligations or responsibilities even where the bank's security system is commercially unreasonable. The court also noted that several material disputes of fact remained to be resolved. For example, Ocean Bank disputes Patco's claim that the unauthorized transfers were caused by malware and keylogging. Ocean Bank argues that Patco cannot prove that its security credentials were misappropriated in a keylogger attack because Patco had scrubbed its computers before a forensic specialist could analyze the computers and locate any potentially responsible malware. To the extent the case proceeds to trial, it is likely Ocean Bank will argue that Patco is responsible for its losses because it lost its credentials through its own negligence or the negligence of its employees. The First Circuit observed, however, that given the relatively modest amount at stake, and the substantial issues to be resolved, the parties would be wise to devote their resources to achieving a settlement.

The legal analysis in Patco, involving a small customer and modest losses, is equally applicable to much larger and more sophisticated customers with the potential for much larger losses. Given that the First Circuit is the first federal appellate court to speak authoritatively on the subject, the First Circuit's interpretation of the "commercially reasonable" test is likely to reverberate far beyond the borders of the First Circuit. For that reason, all commercial banks should take heed and review their security procedures. Security systems that merely rely on asking customers for IDs, passwords, and challenge questions are clearly insufficient. Additional layers, such as password tokens and customer verification, should be considered. Above all, banks need to design platforms that seek input about each customer's particular circumstances, and the available security procedures should effectively utilize that customer information. By requiring more input from their customers, banks may also be able to shift some responsibility back to the customer.

About Scott O'Connell

Partner | Nixon Peabody | Boston, MA
617.345.1150 | soconnell@nixonpeabody.com

Scott O'Connell is deputy chair of Nixon Peabody's Litigation department as well as the practice group leader of the Commercial Litigation team and the Class Action & Aggregate Litigation team. He represents integrated financial service companies—including banks, securities firms, insurance companies, and regulated subsidiaries of nonfinancial parents—in federal and state court litigation and before regulatory agencies.

Scott has extensive experience defending financial institutions in class actions concerning lender liability, breach of contract, breach of fiduciary duty, breach of good faith, unfair and deceptive trade practices, fraud, misrepresentation, fair debt collection practices, and civil RICO. He has particular trial experience litigating complex financial relationships between parties, unfair and deceptive trade practices claims, corporate control issues including corporate freeze-out, lender liability, and civil RICO.

While at law school, Scott served as an editor of the Cornell Law Review and as chancellor of the Moot Court Board. He was also an instructor in the Cornell undergraduate government course, "Law: Its Nature and Function."

Recognition

Scott has been recognized for exceptional standing in the legal community in Chambers USA: America's Leading Lawyers for Business 2011 for litigation work. He has also been recognized by Chambers USA in previous years. In addition, he has been recognized as a "New England Super Lawyer" in Securities Litigation based on a peer-review survey by Boston Magazine (2007 to present) and has been included in The Best Lawyers in America 2010 and 2011 in Commercial Litigation (Copyright 2009 by Woodward/White, Inc., of Aiken, SC). Scott has earned an AV peer rating from Martindale-Hubbell.

Affiliations

Scott is currently a member of the Federal Court Advisory Committee for the District of New Hampshire. In January 2003, he was selected by New Hampshire state-wide paper, The Union Leader—as one of the state's "Forty under 40." Scott is a former vice chairman of the Farnum Center, a statewide alcohol and drug in-patient recovery program; former member of the Board of Directors of the New Hampshire Food Bank (a program of Catholic Charities); past president of the New Hampshire Task Force to Prevent Child Abuse; former captain, Heritage United Way Community Investment Process; founding director of the St. Lawrence University Alumni Lawyers Association; and New Hampshire coordinator of the Cornell Law School Alumni Association. Mr. O'Connell is a graduate of Leadership New Hampshire.

Education

- Cornell Law School, J.D., 1991, (Editor, Law Review)
- St. Lawrence University, B.A., 1987, cum laude
- Harvard Business School, 2008, "Leading Professional Service Firms"