FOR PUBLICATION

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

FEDERAL TRADE COMMISSION, *Plaintiff-Appellee,* v. NEOVI, INC., DBA Neovi Data Corporation, DBA Qchex.com; G7 PRODUCTIVITY SYSTEMS, INC., DBA Qchex.com; JAMES M. DANFORTH, individually, and as an officer of Neovi, Inc. and G7 Productivity Systems, Inc.; THOMAS VILLWOCK individually, and as an officer of Neovi, Inc., *Defendants-Appellants.*	No. 09-55093 D.C. No. 3:06-cv-01952-JLS-JMA OPINION

Appeal from the United States District Court
for the Southern District of California
Janis L. Sammartino, District Judge, Presiding

Argued and Submitted
March 4, 2010—San Diego, California

Filed May 14, 2010

Before: Michael Daly Hawkins, Sidney R. Thomas, and
M. Margaret McKeown, Circuit Judges.

Opinion by Judge McKeown

COUNSEL

Michael L. Mallow (argued), Los Angeles, California, for the appellants.

Lawrence DeMille-Wagman (argued), Washington, DC, for the appellee.

OPINION

McKEOWN, Circuit Judge:

The Federal Trade Commission ("FTC") has broad powers under the FTC Act to prevent businesses from engaging in unfair or deceptive practices. 15 U.S.C. §§ 41-58. This case

arises from a website—managed by Neovi Data Corporation (DBA Qchex.com), G7 Productivity Systems (DBA Qchex.com), James Danforth, and Thomas Villwock (together "Qchex")—that created and delivered unverified checks at the direction of registered users. During its six-year run, fraudsters and con artists extensively abused the website.

We examine here the reach of § 5 of the Act, which empowers the FTC to prevent the use of "unfair methods of competition in or affecting commerce . . . ." 15 U.S.C. § 45(a)(1). The key issue on appeal is whether Qchex is liable for causing substantial injury to consumers that is not reasonably avoidable or outweighed by countervailing benefits. 15 U.S.C. § 45(n). The district court granted summary judgment in favor of the FTC, finding that Qchex's profound lack of diligence, coupled with the affirmative acts of creating and delivering hundreds of thousands of unverified checks—over 150,000 of which were from accounts later frozen for fraud—warranted liability under the Act. Qchex was ordered to disgorge $535,358 in revenue and permanently enjoined from operating any similar business without taking appropriate, specified measures to protect consumers. We affirm.

BACKGROUND

I. QCHEX.COM

From 2000 to 2006, Qchex marketed a series of software programs on a website called "Qchex.com." The software allowed registered users to create and send checks by post or email. In October 2006, the website was shut down. The governing corporation, Neovi,[1] filed for Chapter 11 bankruptcy a year later in October 2007.[2]

[1]James Danforth was the Vice President, Chief Operating Officer, Treasurer, Secretary, and registered service agent of Neovi. Thomas Villwock was the owner, Chief Executive Officer, and President of Neovi.

[2]After Qchex was shut down, but before filing for bankruptcy, Neovi offered a similar check creation and delivery service called "Gochex." After filing for bankruptcy, Villwock and Danforth established iProlog Corporation and launched a third check delivery service called "Free-Quickwire.com." iProlog hired all Neovi employees and conducted the same business activities.

To register for a Qchex account, users were prompted to enter a name and email address, and then to create a password. The account could be activated simply by clicking on a link that Qchex sent to the email address provided. Setup was completed after Qchex received pertinent information about the user's bank account, such as the routing and account numbers. Registered users could submit a request on the website that a check drawn from their account be created and delivered to a third party. To achieve this end, users needed only to enter the name of a payee, the check amount, and the payee's email or mailing address, depending on the preferred method of delivery. Qchex.com then converted the information into a negotiable instrument that, when printed, conformed to U.S. banking regulations. The instrument was designed to be negotiable without the user's signature, but users could choose to upload their signatures if they so desired.

If the user chose to send the check electronically, the payee would receive email instructions to sign up for an account on Qchex.com. Once registered, the payee could print the check, and a confirmation email would be sent to the "payor."[3] If the user chose to send the check by post, it would be printed at a "print service center" operated in the main by employees of G7 Productivity Systems, a California corporation that produced the check software, ink, and paper that was marketed by Neovi on the Qchex website.[4] G7 employees mailed the checks to the payees.

[3]Electronically delivered checks could only be printed using special ink and paper; these items were advertised and offered to the payee in the notification email.

[4]Danforth is G7's Executive Vice President, Chief Financial Officer, Secretary, and registered service agent. Villwock is a business consultant at G7 but considered by its employees to be the de facto President.

II. FRAUD

The Qchex system was highly vulnerable to con artists and fraudsters. Because the information necessary to set up an account was relatively public and easy to come by, it was a simple matter for unscrupulous opportunists to obtain identity information and draw checks from accounts that were not their own. Indeed, over a six-year period, Qchex froze over 13,750 accounts for fraud. Those accounts spawned nearly 155,000 checks, supplied over 37,350 bank account numbers, and were the source of checks totaling more than $402,750,000—an amount more than half of the total drawn during that time.

As one would expect, Qchex received hundreds of letters and thousands of telephone calls from consumers, banks, and law enforcement agencies complaining about funds drawn from accounts without authorization. Victims included not only individuals and businesses, but also large institutions and agencies like the University of Chicago, Goldman Sachs, the Federal Communications Commission, and, ironically, the FTC itself.

Qchex contends that it was attuned to the risk of fraud from the outset and acted responsibly to curtail it. Before 2005, Qchex argues that it took multiple fraud reduction measures, pointing specifically to the "Qchex Monitor" system that enabled employees to spot irregular activity like the presence of large volumes of high-denomination checks. Internet Protocol addresses associated with fraudulent transactions were blacklisted and Qchex placed warnings on the checks alerting the payees that it could not verify whether the check was duly authorized by the payors. On a case-by-case basis, Qchex froze suspicious accounts. Finally, Qchex encrypted the check data it transmitted over the Internet and used barcoding to obscure account data on the face of the checks it issued.

None of these measures proved successful. The Qchex Monitor was underutilized and does not appear to have been

employed in any focused way to target or unearth fraud. The rest of the measures were either reactive—taking place after fraud had already occurred—or unresponsive to the chief concern that checks were being drawn against unauthorized accounts.

In 2005, after meeting with the American Banking Association and the Federal Deposit Insurance Corporation, Qchex implemented a "micro-deposit" program called the "Qchex Validation System" ("QVS"). To verify that a user's account was legitimate, Qchex made a single, nominal deposit of somewhere between three and twenty cents in the account the user provided. The user was required to check the account to determine the deposit's value. Qchex declined to deliver checks from a provided account unless the user was first able to accurately report the value of the micro-deposit. After three failed attempts, the Qchex account would be frozen.

Although it was a step in the right direction, QVS had a number of loopholes that rendered it ineffective. For example, it only applied to accounts that were newly activated. Users who had balances established before the new security system was adopted were still able to send checks by mail. Even for new users the system was easy to game. Because QVS validated just one bank account per registered user, as long as a user had legitimate access to one bank account, other accounts —possibly unauthorized—could be used without verification through QVS. Significantly, the new system did not apply to emailed checks at all. Whatever its failings, the QVS system was short lived. For reasons that are unclear, the payment processor that enabled Qchex to run the system terminated its contract in April 2006.

ANALYSIS

I. UNFAIR PRACTICES UNDER § 5 OF THE FTC ACT

[1] Under § 5 of the FTC Act, an unfair practice or act is one that "causes or is likely to cause substantial injury to con-

sumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

A. Causation

The district court found that Qchex is liable for the "[u]nfair creation and delivery of unverified checks." Qchex urges that this charge is both "legally" and "literally" impossible. It claims that only *users* can create checks because "without user input nothing, and certainly not a check, . . . could be created or delivered." This semantic argument is meant to encompass not only the causation requirement, but also Qchex's claim that it was not given adequate notice of the charges.

[2] Qchex's challenge to causation is best captured in its statement that it did not "obtain, input or direct" the delivery of consumer information nor facilitate the theft. This spin ignores the fact that Qchex created and controlled a system that facilitated fraud and that the company was on notice as to the high fraud rate. Qchex's approach would immunize a website operator that turned a blind eye to fraudulent business made possible only through the operator's software. Even if the creation of the checks was impossible without user input, that does not mean Qchex did not create the checks that it later delivered.

By Qchex's logic, a publishing house cannot be said to create and distribute books, because it is impossible to print books without content provided by an author. Indeed, the creation and distribution of most any good is subject to a host of sequential steps. Some of those steps involve the contribution of independent causal agents, but those contributions do not magically erase the role of the aggregator and distributor of the goods. This reality becomes obvious if we flip the counterfactual. Without the Qchex software and the G7 workforce, *users* would not be able to create and deliver checks. There-

fore, by Qchex's lights, users cannot be said to create and deliver checks either. This circular logic leads to the absurd result that although checks have been created and delivered, no one is doing the creating or the delivering.

[3] At most, Qchex's argument shows that Qchex and the users each contributed to the creation and delivery of the checks. But, even granting this characterization, Qchex is not discharged from liability under the FTC Act—a single violation of the Act may have more than one perpetrator. *See, e.g.*, *FTC v. Bay Area Bus. Council, Inc.*, 423 F.3d 627, 630 (7th Cir. 2005) (holding multiple defendants liable under § 5 of FTC Act).

[4] To support its argument that the FTC's showing of causation was insufficient, Qchex urges us to seek interpretive guidance from several California state cases that were decided under California Business & Professions Code § 17200—the so-called "Little FTC Act." We decline the invitation. While it is common practice for states with consumer protection statutes modeled on the FTC Act to rely on federal authority when interpreting those statutes, the reverse is not the case. As the FTC points out, given the abundance of state laws on which such interpretations could be based, this practice would likely result in a sea of inconsistent rulings. *See Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1363 (11th Cir. 1988) (noting that there is nothing constraining the FTC "to follow judicial interpretations of state statutes in construing the agency's section 5 authority").

Qchex also criticizes the district court's reliance on two unpublished district court cases. Although not precedential, these cases are instructive insofar as they illustrate the role of a facilitator under the FTC Act.

In *FTC v. Windward Marketing, Ltd.*, the court found multiple defendants liable for a magazine telemarketing scheme in which defendants obtained victims' banking information

over the phone and illegitimately debited their accounts for magazine subscriptions they did not realize they were purchasing. Defendant Wholesale Capital Corporation ("Wholesale") maintained several bank accounts used to collect on victims' invoices. *See* No. Civ.A. 1:96-CV-615F, 1997 WL 33642380, at *11-*12 (N.D. Ga. Sept. 30, 1997). The court noted that 40% of the drafts were returned unauthorized and that, at the very least, Wholesale was "on notice of a high probability of fraud and/or unfairness . . . ." *Id.* at *13.

Although Wholesale did not itself make any misrepresentations or initiate the fraudulent scheme, the court found Wholesale liable under the FTC Act because it "facilitated and provided substantial assistance to [a] . . . deceptive scheme," resulting in substantial injury to consumers. *Id.* at *12-*13. This conduct was enough to find Wholesale primarily liable—as opposed to liable as an accomplice—under the Act. *Id.*

Similarly, in *FTC v. Accusearch, Inc.*, Accusearch was held liable for maintaining a website that sold the GPS locations of individual cell phones and other confidential, personal information, even though it did not itself illegally obtain the information. No. 06-CV-105-D, 2007 WL 4356786, at *6 (D. Wyo. Sept. 28, 2007) (noting that "[e]ach time the Defendants placed an order for phone records, they caused others to use false pretenses and other fraudulent means to obtain confidential consumer phone records").

[5] These cases illustrate that businesses can cause direct consumer harm as contemplated by the FTC Act in a variety of ways. In assessing that harm, we look of course to the deceptive nature of the practice, but the absence of deceit is not dispositive. Nor is actual knowledge of the harm a requirement under the Act. Courts have long held that consumers are injured for purposes of the Act not solely through the machinations of those with ill intentions, but also through the actions of those whose practices facilitate, or contribute to, ill intentioned schemes if the injury was a predictable con-

sequence of those actions. *See FTC v. Winsted Hosiery Co.*, 258 U.S. 483, 494 (1922) (holding that "[t]he honest manufacturer's business may suffer, not merely through a competitor's deceiving his direct customer, the retailer, but also through the competitor's putting into the hands of the retailer an unlawful instrument . . ."); *FTC v. R.F. Keppel & Bro., Inc.*, 291 U.S. 304, 314 (1934) (holding candy retailer liable for unfair practices although manufacturer was responsible for the element of chance that made the practices unfair); *Regina Corp. v. FTC*, 322 F.2d 765, 768 (3d Cir. 1963) (explaining that "[w]ith respect to those instances where petitioner did not contribute to the [misleading act], it is settled that [o]ne who places in the hands of another a means of consummating a fraud or competing unfairly in violation of the Federal Trade Commission Act is himself guilty of a violation of the Act") (quotation marks and citations omitted).

Qchex had reason to believe that a vast number of checks were being drawn on unauthorized accounts—checks that it legitimized in the eyes of consumers. Aside from the prodigious number of complaints Qchex received, its president testified that Qchex expected the site would be used for fraudulent purposes from the beginning. Qchex nonetheless continued to create and deliver checks without proper verification. By doing so it engaged in a practice that facilitated and provided substantial assistance to a multitude of deceptive schemes.

[6] To be clear, none of this is to say that Qchex is liable under a theory of aiding and abetting. Qchex engaged in behavior that was, *itself*, injurious to consumers. Qchex's business practices might have served to assist others in illicit or deceptive schemes, but the liability under the FTC Act that attaches to Qchex is not mediated by the actions of those third parties. Qchex caused harm through its own deeds—in this

case creating and delivering unverified checks—and thus § 5 of the FTC Act easily extends to its conduct.[5]

[7] Finally, as to its notice argument, Qchex contends that the FTC's complaint must be read as alleging that Qchex "originated" checks in the sense that it, not the users, directed the unauthorized withdrawal of funds out of consumer accounts. This allegation does not square with a plain reading of the complaint. As the district court points out, Qchex created the checks in the sense that it physically brought them into being—or provided the means to do so—and made them appear legitimate and credible in the eyes of consumers.

B. Substantial Injury

[8] The FTC met its burden of establishing substantial injury; there is no triable issue of fact with respect to this issue. The district court based its findings on record facts that it pulled from various sources, including Qchex's database, Qchex's declarations, and consumer complaints. Qchex's claim that the district court based its findings on "speculation, not evidence," is without support.

The district court acknowledged that the number of fraudulent items created could not be definitively quantified, but it also said that more than half the total value of all the checks drawn with the help of Qchex came from accounts later frozen for fraud. That concrete and quantifiable finding is sufficient to show substantial harm because it establishes that consumers "were injured by a practice for which they did not bargain." *See Windward Marketing*, 1997 WL at *11 (citing

[5]Although we grant Qchex's motion to take judicial notice of various congressional documents that support in some measure Qchex's claim that aiding and abetting liability is not cognizable under the FTC Act, the documents have little bearing on the outcome of this appeal. Qchex's actions caused consumer harm; it did not merely aid or abet others who caused consumer harm. We take no position on aiding and abetting liability under the Act.

Orkin Exterminating Co., 849 F.2d at 1364-65). An act or practice can cause "substantial injury" by doing a "small harm to a large number of people, or if it raises a significant risk of concrete harm." *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 972 (D.C. Cir. 1985) (quotation marks and citations omitted) *cert. denied*, 475 U.S. 1011 (1986).

Finally, in an effort to skirt liability, Qchex observes that because the victims of fraud already had their banking information compromised, they would have had to spend time protecting their accounts whether or not the Qchex system was instrumental in their loss. If Qchex caused or helped to cause substantial injury to consumers, it is no defense to say that consumers nonetheless would have been harmed by someone else. In any case, it is not clear that the fraudsters would have had the means to take advantage of the victims' information without the aid of the Qchex software. Indeed, some of the frauds stemming from the Qchex system involved victims whose account information was not compromised.[6]

C. Reasonable Avoidability

[9] In determining whether consumers' injuries were reasonably avoidable, courts look to whether the consumers had a free and informed choice. *See Am. Fin. Servs. Ass'n*, 767 F.2d at 976. Qchex argues that there are triable issues of fact as to whether consumers could reasonably have avoided their

[6]Consider the following example found in the record: A confidence man made contact with a woman over the Internet and gained her trust. He represented himself as a wealthy individual and told the woman that he had asked an acquaintance who owed him money to make a check out directly to her as a gift. The woman subsequently received a (Qchex) check in the mail from an unrecognized name in the amount of $4,000. She protested to the con man that the gift was too generous and he suggested that she therefore keep $1,000 and wire the other $3,000 to a friend traveling in Nigeria who had lost his luggage. She did so. The check, of course, was illegitimate and the woman was on the hook for the $3,000 sent to Nigeria and the bank fees incurred for an overdrawn account.

alleged injuries. Although the district court addressed consumers' ability to avoid injury before it occurred, Qchex argues that the court did not address the consumers' ability to mitigate damage after it occurred. *See Orkin Exterminating Co.*, 849 F.2d at 1365 (discussing both anticipatory and subsequent mitigation). Qchex maintains that even if consumers were substantially injured, they were able to take "reasonable steps to avoid loss" by communicating with their banks after the unauthorized payments were discovered.

[10] The district court sufficiently addressed both avenues of mitigation. In denying Qchex's reconsideration motion, the court wrote:

> It is likely that some consumers never noticed the unauthorized withdrawals. Even if the consumer did notice, obtaining reimbursement required a substantial investment of time, trouble, aggravation, and money. Further, Defendants' uncooperativeness only increased this outlay. Neither could consumers mitigate the period of time during which they lost access to and use of the funds taken using Defendants' fraudulent checks. Regardless of whether a bank eventually restored consumers' money, the consumer suffered unavoidable injuries that could not be fully mitigated.

Qchex has not shown that there is a material issue of fact as to whether consumer injuries were reasonably avoidable on either end of the fraudulent transactions.

D. No Substantial Consumer Benefit

[11] The FTC also met its burden of showing that consumer injury was not outweighed by countervailing benefits to consumers or to competition. The FTC offered the declaration of a law professor who has written extensively about electronic commerce, credit cards, and payment systems in

support of its claim. The FTC's expert explained that the Qchex website is of limited use to an ordinary consumer because "all large banks," offer the same services at a cheaper price and with greater security. He also noted the presence of other third parties in the marketplace—like PayPal—that provide similar services. Even though Qchex's email service was relatively unique, it was considerably less convenient given that many commercial payees do not accept emailed checks. There is also a disincentive to use the email method because it is more costly to the recipient who must buy special ink, paper, and a suitable printer to accept emailed checks.

The district court found that Qchex failed to counter the FTC expert's testimony. Qchex put forward a short declaration from one of its executives purporting to do so, but the district court found that the declaration was "the epitome of uncorroborated and self-serving testimony," and declined to rely on it to find a genuine issue of fact. As a result, Qchex accuses the district court of improperly weighing evidence and making findings of fact.

Specific testimony by a single declarant can create a triable issue of fact, but the district court was correct that it need not find a genuine issue of fact if, in its determination, the particular declaration was "uncorroborated and self-serving." *See Villiarimo v. Aloha Island Air, Inc.*, 281 F.3d 1054, 1061 (9th Cir. 2002). The district court was on sound footing concluding that Qchex put forward nothing more than a few bald, uncorroborated, and conclusory assertions rather than evidence.

II. EQUITABLE RELIEF[7]

[7]We decline to consider Qchex's argument, based on *FTC v. Verity Int'l, Ltd.*, 443 F.3d 48, 67 (2d Cir. 2006), that the district court lacked jurisdiction or authority to award damages or disgorgement under § 13(b) of the FTC Act. Qchex did not properly raise this issue in the district court, and thus the argument is waived on appeal. *See In re E.R. Fegert, Inc.*, 887 F.2d 955, 957 (9th Cir. 1989) (explaining that appellate courts will not consider an argument unless it has been "raised sufficiently for the trial court to rule on it").

[12] Analogizing to securities law, the district court concluded that the appropriate measure of equitable disgorgement was Neovi's total revenue. *See SEC v. JT Wallenbrock & Assocs.*, 440 F.3d 1109, 1113 (9th Cir. 2006) (explaining that "the district court has broad equity powers to order the disgorgement of 'ill-gotten gains' obtained through the violation of federal securities laws") (internal citations omitted).[8] An evidentiary hearing was unnecessary because there were no "genuine issues of material fact remaining in the case." Qchex argues that this conclusion was error in that "the FTC did not put forth admissible evidence demonstrating that Neovi realized $535,358 in 'ill gotten gains.' " The district court derived this specific figure from the gross receipts on Neovi's tax return, the details of which were not disputed.[9] Qchex argues that the figure is invalid because Qchex's revenues were exceeded by developing, maintenance, and operating costs for the software and website.

Qchex's argument is puzzling. The court explicitly declined to reduce the disgorgement by the cost of developing and maintaining the Qchex system because those activities "facilitated and contributed to the check fraud," and because Qchex did "not offer evidence showing exact costs or expenses which the Court could reasonably use in its calculations." It

[8]In *Wallenbrock* we stressed that in making this calculation, the court has 'broad discretion,' and needs only a 'reasonable approximation of profits causally connected to the violation . . . . [D]isgorgement should include all gains flowing from the illegal activities." 440 F.3d at 1113-14.

[9]The district court found that the tax returns were properly authenticated based on an executive's declaration submitted in a supplemental brief. Before the district court, Qchex did not contest the authenticity of the tax returns or the veracity of the declaration. Instead, Qchex argued that the manner of authentication (as an exhibit to a supplemental reply brief) was improper. The district court did not abuse its discretion on this evidentiary point and resolution of this issue would not be aided by an evidentiary hearing. To the extent Qchex now challenges the authenticity of the tax returns, that issue is not properly before us on appeal. *See In re E.R. Fegert, Inc.*, 887 F.2d at 957.

is unclear what facts could be uncovered at an evidentiary hearing that Qchex did not have the opportunity to present to the district court. In any case, as the FTC points out, the disputed points appear to be questions of law, not of fact.

III. THE INJUNCTION

[13] Under the injunction order, Qchex is prohibited from "creating or delivering any check for a customer, unless [it] perform[s] the verification procedures identified" in the rest of the order. Qchex characterizes the order as a mandatory injunction, claiming that § 13(b) of the FTC Act does not expressly authorize mandatory injunctions.[10]

[14] According to the most general understanding of the distinction between mandatory and prohibitive injunctions, the district court's order is prohibitory, not mandatory. *See Black's Law Dictionary* 855 (9th ed. 2009) (defining "prohibitory injunction" as an injunction that "forbids or restrains an act," and "mandatory injunction" as an injunction that "orders an affirmative act or mandates a specified course of conduct"). The prohibition contains an exception, but this language does not convert it from a prohibitory to a mandatory injunction; Qchex is not ordered to undertake any affirmative action.

AFFIRMED.

[10]We need not address the availability of mandatory injunctions under § 13(b) of the FTC Act.