PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNSPAM TECHNOLOGIES, INC., d/b/a Project Honey Pot; JOHN DOE, on behalf of himself and all others similarly situated,
Plaintiffs-Appellants,

v.

ANDREY CHERNUK, d/b/a Toronto Pharmacy; BORIS LIVSHITS, d/b/a Toronto Pharmacy; ZAO RAIFFEISENBANK; BANK STANDARD COMMERCIAL BANK CLOSED JOINT-STOCK COMPANY; AZERIGAZBANK; DNB NORD BANKA,
Defendants-Appellees,

and

JOHN DOE(S), Injuring PHP and its Members by Harvesting Email Addresses, and Transmitting Spam; ST. KITTS-NEVIS-ANGUILLA NATIONAL BANK LIMITED; RIETUMU BANK,
Defendants.

No. 11-2406

Appeal from the United States District Court
for the Eastern District of Virginia, at Alexandria.
Leonie M. Brinkema, District Judge.
(1:11-cv-00015-LMB-JFA)

Argued: January 30, 2013

Decided: May 3, 2013

Before NIEMEYER, SHEDD, and AGEE, Circuit Judges.

Affirmed by published opinion. Judge Niemeyer wrote the opinion, in which Judge Shedd and Judge Agee joined.

COUNSEL

ARGUED: Jon Linden Praed, INTERNET LAW GROUP, Arlington, Virginia, for Appellants. Craig Brian Whitney, MORRISON & FOERSTER, LLP, New York, New York, for Appellees. **ON BRIEF:** Jennifer Ancona Semko, Edwin B. Swan, BAKER & MCKENZIE, LLP, Washington, D.C., for Appellees Bank Standard Commercial Bank Closed Joint-Stock Company and Azerigazbank; Andrew P. Sherrod, HIRSCHLER FLEISCHER, PC, Richmond, Virginia, Owen J. McKeon, GIBBONS PC, Newark, New Jersey, for Appellee ZAO Raiffeisenbank; James E. Hough, MORRISON & FOERSTER, LLP, New York, New York, for Appellee DNB Nord Banka.

OPINION

NIEMEYER, Circuit Judge:

The issue presented in this appeal is whether the district court erred in dismissing a complaint against four foreign banks for lack of personal jurisdiction. The complaint alleges an international conspiracy of foreign banks, corrupt Internet Payment Service Providers, and illegal prescription drug dealers ("pharmacists") to sell illegal prescription drugs over the Internet.

One plaintiff, John Doe, an Arlington, Virginia resident, purchased prescription drugs online from the "Canadian Phar-

macy," paying for the drugs with his Visa debit card. When the drugs never arrived, he canceled the transaction at his United States-based bank that issued his debit card, and the bank refunded his payment. Thereafter, he received a voluminous number of spam emails for prescription drugs. And the other plaintiff, Unspam Technologies, Inc., doing business as Project Honey Pot (hereafter "Project Honey Pot"), is a Delaware corporation that was formed to pursue the enforcement of Internet spam laws by tracing and identifying spam emails, including solicitations for illegal prescription drugs.

The plaintiffs commenced this case as a putative class action, naming as defendants two "pharmacists," who were Russian citizens, and six foreign banks. They alleged that the defendants participated in a global Internet conspiracy to sell illegal prescription drugs, in violation of the laws of the United States and Virginia. The two pharmacists were dismissed, one voluntarily and the other for lack of service, and two of the six banks were also dismissed voluntarily. The district court dismissed the other four banks for lack of personal jurisdiction.

Challenging the dismissal of the four banks on appeal, the plaintiffs contend that the district court erred in failing to recognize that, because the banks were alleged to be part of a global conspiracy, any single member's constitutionally sufficient contacts with Virginia would subject every coconspirator to personal jurisdiction in Virginia. The plaintiffs, however, rest application of their theory of jurisdiction on only supposition and speculation about a conspiracy and the grossly attenuated contacts of its members with Virginia. Therefore, they have failed to show that any of the banks has constitutionally sufficient contacts with Virginia, or with the United States, to subject them to personal jurisdiction in a court in Virginia. Accordingly, we affirm.

I

In October 2007, John Doe attempted to buy prescription drugs from an online pharmacy called "Canadian Pharmacy."

He paid for the drugs with his Visa debit card, issued to him by a United States-based bank. After several weeks, when Doe had not received his drugs, he attempted to contact the pharmacy directly, but was unsuccessful. He then notified his bank, which credited his account for the full purchase price and assigned him a new Visa debit card. Since that transaction, Doe claims that he has received a voluminous number of spam emails.

Project Honey Pot maintains a network of spam-tracking "honey pots," with the sole purpose of tracking and identifying spam emails in an effort to combat such emails. It claims that its network has "allow[ed] spammers, phishers, and other e-criminals to be tracked throughout their entire 'spam life cycle.'" Project Honey Pot claims to have processed, on its Virginia servers, spam emails from online pharmacies associated with a global conspiracy to sell illegal prescription drugs over the Internet.

Project Honey Pot and Doe commenced this action, seeking an injunction against spam email that solicits illegal prescription drugs, as well as damages, and claiming that "[l]awsuits of this kind are another effective way of deterring harvesters [of email addresses] and the spammers who buy their harvested email lists." Project Honey Pot states that since it started collecting data in 2004, it has "identified over 80 million spam servers, over 96 thousand harvesters [of email addresses], over 14 million dictionary attackers, and since April 2007, has identified over 348 thousand comment spam server IP addresses."

The plaintiffs claim, based on Internet research conducted by it and others and the comparison of telephone numbers and transaction identifiers, that the defendant pharmacists Andrey Chernuk and Boris Livshits were behind "Canadian Pharmacy." They allege that Chernuk and Livshits used not only "Canadian Pharmacy" but other similar trade names to solicit the sale of illegal prescription drugs—sales made without

valid prescriptions and sales of counterfeit drugs marketed with false advertising. The plaintiffs also claim that the defendant pharmacists have a relationship with a Russian-based Internet Payment Service Provider called Chronopay and that Chronopay, in turn, has contracts with various banks throughout the world to process Internet credit card transactions. While the international Visa network includes thousands of banks, the plaintiffs claim that six foreign banks have processed a majority of Chronopay's transactions: St. Kitts-Nevis-Anguilla National Bank Ltd., in St. Kitts; ZAO Raiffeisenbank, in Moscow, Russia; DnB Nord Banka, in Copenhagen, Denmark; Bank Standard Commercial Bank Closed Joint-Stock Company, in Baku, Azerbaijan; Azerigazbank, in Baku, Azerbaijan; and Rietumu Bank, in Riga, Latvia.

Because these banks processed a majority of Chronopay's transactions for illegal prescription drugs without enforcing Visa's stated rules for rejecting such transactions, the plaintiffs allege that the banks are part of a global conspiracy to sell illegal prescription drugs. As the plaintiffs claim, a customer's online Visa charge, such as Doe's charge, is presented by online pharmacists to an Internet Payment Service Provider, such as Chronopay, which in turn presents it to a participating Visa bank (in this case possibly one of the six banks), which then processes the transaction through the international Visa network, ultimately charging the customer's account in his home state (in this case, Virginia). In short, the plaintiffs contend that the banks' participation was essential to the conspiracy.

The plaintiffs' eight-count complaint alleges violations of the False Marking Act, 35 U.S.C. § 292; the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962 *et seq.*; the federal CAN-SPAM Act of 2003, 15 U.S.C. § 7701 *et seq.*; and the Virginia Computer Crimes Act, Va. Code Ann. § 18.2-152.1 *et seq.*; as well as common law claims for conspiracy, negligence, and unjust enrichment.

The plaintiffs voluntarily dismissed St. Kitts-Nevis-Anguilla National Bank and Rietumu Bank. The four remaining banks filed motions to dismiss pursuant to Federal Rules of Civil Procedure 12(b)(2) and 12(b)(5), contending that the court lacked personal jurisdiction over them and that the plaintiffs' service of process on them was ineffective. The district court granted the motions of Bank Standard and Azerigazbank to dismiss under Rule 12(b)(2) for lack of personal jurisdiction by order dated November 18, 2011. Additionally, it granted the plaintiffs leave to file a third amended complaint within 14 days, but the plaintiffs elected not to file one.

A few days after dismissing the two banks, the court ordered the plaintiffs to show cause why the motions to dismiss filed by ZAO Raiffeisenbank and DnB Nord should not also be granted on the same grounds. After briefing, the district court granted these banks' motions to dismiss under Rule 12(b)(2) for lack of personal jurisdiction by order dated December 2, 2011. At the same time, it rejected the plaintiffs' request for jurisdictional discovery.

The plaintiffs filed a notice of appeal from the district court's orders dismissing the four banks for lack of personal jurisdiction. At that point in time, however, the two defendant pharmacists were still in the case. The plaintiffs thereafter voluntarily dismissed Livshits, and the district court dismissed Chernuk because of the plaintiffs' failure to effect timely service on him.

After all defendants had been dismissed, the plaintiffs filed a Rule 59(e) motion on April 23, 2012, asking the court to vacate its order granting the motions of ZAO Raiffeisenbank and DnB Nord to dismiss. They relied, in part, on third-party discovery that they had conducted to bolster their position. The district court denied the motion, finding the following fatal flaws with the plaintiffs' arguments:

> *First*, plaintiffs cannot show that these defendants have had any direct contacts with Virginia. *Second*,

> plaintiffs' "new" evidence still does not link the defendant banks with Virginia customers, Chernuk, Livshits, or the single transaction at issue in this case. *And finally*, even if plaintiffs could show that these banks processed transactions for merchants with Virginia customers, personal jurisdiction would still be improper due to the extremely attenuated nature of the banks' contacts with the forum.

(Emphasis added).

The only issue now before us is whether the district court had personal jurisdiction over the four foreign banks.

II

Project Honey Pot and John Doe are seeking to redress a global cyber-crime conspiracy "to use popular credit card processing systems (particularly the Visa network) to collect funds from the sale of illegal counterfeit prescription drugs over the Internet to American consumers." They allege that American consumers, such as John Doe, have responded to email advertisements for prescription drugs, buying the drugs with credit cards. The Internet "pharmacists" then present the credit card transactions to Internet Payment Service Providers, which in turn present them to foreign banks participating in the international Visa network. The banks collect on the charges from the consumers' accounts through the Visa network. Ultimately, the pharmacists never fill the orders for the prescription drugs or fill the orders with counterfeit drugs. The plaintiffs argue that the frequency and nature of such transactions support their claim as to the existence of a global conspiracy that violates U.S. and Virginia law.

To justify personal jurisdiction over the foreign banks, Project Honey Pot and John Doe contend that the Internet "pharmacists" deliberately transmit spam emails on the Internet, seeking to sell prescription drugs and aiming at email

addresses that have been "harvested" from web pages, including addresses of persons in Virginia, such as John Doe. They argue that, based on this contact with Virginia, the district court has jurisdiction over the pharmacists under Virginia's long arm statute and thus over the pharmacists' coconspirators.

Each of the banks has stated that it does not have any contact with Virginia or the United States. In their affidavits, they claimed that they do not maintain interactive websites marketing services to customers in Virginia; do not engage in the operation of any business venture in Virginia or anywhere in the United States; and do not issue credit cards to customers in the United States. They also claimed, more specifically, that none serves as a merchant bank in the Visa network for any merchants located in Virginia or in the United States and that they do not interact directly with customers of the credit card merchants whom they do serve. Finally, they stated that they have never sent spam email or directed the sending of any spam email.

Although Project Honey Pot and Doe do not attempt to demonstrate that the four banks have done business in Virginia or in the United States or have sent spam emails to Virginia, they claim that the four banks, by processing the pharmacists' transactions on the international Visa network, are coconspirators in a global prescription-drug conspiracy that uses the network. Doe acknowledges that he cannot link his particular purchase to any one of the defendant banks, and similarly, Project Honey Pot does not contend it can directly link the banks with any fraudulent email solicitations for prescription drugs that it received in Virginia. But the plaintiffs explain that they have named these six banks as defendants because they "are responsible for the vast majority of this illegal business extending over a number of years" insofar as they process the largest number of transactions submitted to the Visa network by fraudulent Internet pharmacists. The plaintiffs assert that these banks, "although headquartered out-

side the United States, can be sued in the United States for knowingly participating in a conspiracy that both depends on critical resources within the United States and causes widespread harm to American consumers."

The banks argue that the plaintiffs, in making their conspiracy argument, are relying on "a host of conclusory and hypothetical allegations about a global conspiracy to market and sell pharmaceuticals online, but fail to allege facts sufficient to justify the assertion of personal jurisdiction." As the banks explain:

> At most, plaintiffs' second amended complaint alleges that, because the Banks provide merchant credit card processing services, one of the Banks *may* have provided credit card processing services to an online pharmaceutical merchant, and that merchant *may* have been one of the two individual merchant defendants in this action, who *may* have operated a website accessed by Plaintiff Doe or sent spam e-mail to Project Honey Pot. Plaintiffs do not allege, however, that any of this alleged hypothetical and speculative activity connects the Banks to Virginia.

Personal jurisdiction over persons conducting business on the Internet is determined under a standard that has evolved as necessary to accommodate the nature of the Internet. That standard begins with the principle that the Due Process Clause prohibits a court from exercising personal jurisdiction over a defendant unless that defendant has "certain minimum contacts . . . such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'" *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945) (quoting *Milliken v. Meyer*, 311 U.S. 457, 463 (1940)). Such contacts exist when a defendant "purposely avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its law." *Hanson v. Denckla*,

357 U.S. 235, 253 (1958); *see also Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985) ("This 'purposeful availment' requirement ensures that a defendant will not be haled into a jurisdiction solely as a result of 'random,' 'fortuitous,' or 'attenuated' contacts"). Thus, a defendant outside the forum State must have at least "aimed" its challenged conduct at the forum State. *Calder v. Jones*, 465 U.S. 783, 789 (1984).

Tailoring these principles to electronic Internet activity, we have adopted a three-part inquiry to determine whether a defendant is subject to jurisdiction in a State because of its electronic transmissions to that State. The inquiry considers: "(1) the extent to which the defendant purposely availed itself of the privilege of conducting activities in the State; (2) whether the plaintiffs' claims arise out of those activities directed at the State; and (3) whether the exercise of personal jurisdiction would be constitutionally reasonable." *ALS Scan, Inc. v. Digital Serv. Consultants, Inc.*, 293 F.3d 707, 712 (4th Cir. 2002) (internal quotation marks and alteration omitted). The flexibility of these factors allows a court to focus its attention on the ultimate question of whether a defendant, through its actions, has subjected itself to the sovereignty of the State such that a court in the State can lawfully subject that defendant to a judgment. *See J. McIntyre Mach., Ltd. v. Nicastro*, 131 S. Ct. 2780, 2789 (2011) (Kennedy, J., plurality opinion) ("This Court's precedents make clear that it is the defendant's actions, not his expectations, that empower a State's courts to subject him to judgment").

In this case, there is no indication that any of the four banks acted in such a way as to subject itself to the sovereign power of a court in Virginia. Not one of the banks directed its business to Virginia or aimed its commercial efforts at customers in Virginia. Indeed, there is no evidence that any drug transactions involving the plaintiffs were connected by intermediaries to these banks.

Moreover, even if we were to assume that Doe's purchase was presented by some Internet "pharmacist" to one of the foreign banks for processing through the international Visa network, that transaction still would be too remote an act to justify jurisdiction in Virginia. The transaction would have occurred in the foreign country where the pharmacist presented the Visa charge to the bank, and thereafter, the bank would simply have collected the charge through the Visa network. The foreign bank's relevant activity would thus be localized to the foreign country where it did business, and its only conduct "aimed" from that location would be the transmittal of the transaction into the Visa network. The fact that the transaction ultimately rippled through other countries for the collection of monies would not indicate that the bank purposefully availed itself of the laws of the countries where subsequent transactions occurred. *Cf. ALS Scan*, 293 F.3d at 714 (holding that a Maryland court could not exercise personal jurisdiction over a "passive" Internet service provider when that Internet service provider only enabled the tortfeasor "to create a website and send information over the Internet").

Project Honey Pot and Doe's argument, however, relies on a "conspiracy theory of jurisdiction," under which the banks are imputed with constitutionally sufficient contacts with Virginia through the actions of their alleged coconspirators, namely the Internet "pharmacists" who solicited the fraudulent purchases. To succeed on this theory, the plaintiffs would have to make a plausible claim (1) that a conspiracy existed; (2) that the four bank defendants participated in the conspiracy; and (3) that a coconspirator's activities in furtherance of the conspiracy had sufficient contacts with Virginia to subject that conspirator to jurisdiction in Virginia. *See Lolavar v. de Santibanes*, 430 F.3d 221, 229 (4th Cir. 2005); *McLaughlin v. McPhail*, 707 F.2d 800, 807 (4th Cir. 1983) (per curiam). To satisfy these requirements, the plaintiffs would have to rely on more than "bare allegations." *Lolavar*, 430 F.3d at 229 (internal quotation marks omitted); *see also Jungquist v. Sheikh Sultan Bin Khalifa Al Nahyan*, 115 F.3d 1020, 1031 (D.C.

Cir. 1997) ("[T]he plaintiff must plead with particularity the conspiracy as well as the overt acts within the forum taken in furtherance of the conspiracy" (internal quotation marks omitted)).

In this case, the plaintiffs alleged that Doe entered into a fraudulent transaction online with "Canadian Pharmacy" to purchase prescription drugs and that he paid for the drugs with his Visa debit card. They suggest that two pharmacists in Russia may have been behind the sale, even though they voluntarily dismissed one of the pharmacists later because it turned out that he was not involved, and the district court dismissed the other for a lack of service. Thus, Doe acknowledges that he does not know who engaged him in the transaction or whether any of the four banks processed his Visa charge. The plaintiffs do, however, posit how the banks might be involved.

Through blog research and Internet searches, they have suggested that "Canadian Pharmacy" was a trade name providing a front for the two defendant pharmacists to engage in an Internet conspiracy to deal illegally in prescription drugs. By linking telephone numbers and transaction identifiers, the plaintiffs have suggested that many of the illegal transactions identified "have a connection to Chronopay [the PayPal of Russia] or its two Russian co-founders, Pavel Vrublevsky and Igor Gusev." They are unable, however, to allege that Chronopay was actually involved in Doe's transaction. Rather, they claim that computer science research has linked many fraudulent prescription drug transactions with Chronopay and that Chronopay has processed its transactions through various banks in the international Visa network, but mostly through the four banks at issue here. Thus, they speculate that Doe's transaction could well have been presented by Chronopay to one of the defendant banks. They implicate the banks by the frequency with which they processed such transactions and their alleged failure to apply Visa's operating regulations

to monitor their merchants and "terminate merchants obviously engaged in illegal activity."

The plaintiffs' speculation about the processing of Doe's transaction, however, amounts to no more than a bare allegation or logical possibility and does not suffice to allege a plausible claim of the existence of a conspiracy. Even if we were to assume that Doe's transaction was presented by Chronopay to one of the defendant banks, the plaintiffs still have not alleged sufficient facts to show that the defendant banks participated in the alleged conspiracy. The facts on which they rely could equally describe arms-length transactions involving the presentation of credit card transactions to banks for collection through the Visa network in the ordinary course of business.

Also, the plaintiffs have provided no plausible basis to connect the banks to the spam emails complained of specifically by Project Honey Pot. The only evidence in the record on this claim is provided by affidavits from the banks stating that they never attempted to directly market themselves in the United States, through spam emails or otherwise. The only alleged connection between the banks and spam emails is the overly general allegation that the banks, by processing transactions generated by spam emails, has kept the spammers in business. But conspiracy requires a "common plan," and here there are no allegations that the bank's processing of the transactions were designed to achieve the illegal ends of the fraudulent pharmacists. *See, e.g.*, *Lolavar*, 430 F.3d at 230 (noting the "common plan" requirement) (quoting *First Chicago Int'l v. United Exch. Co.*, 836 F.2d 1375, 1378 (D.C. Cir. 1988)).

In short, the plaintiffs' allegations of conspiracy are conclusory and speculative and do not satisfy the requirements for establishing a conspiracy theory of personal jurisdiction.

III

Project Honey Pot and Doe also argue that personal jurisdiction over the four banks is appropriate under Federal Rule of Civil Procedure 4(k)(2), which permits a federal court to assert jurisdiction in cases "aris[ing] under federal law" when the defendant is not subject to personal jurisdiction in a state court but has contacts with the United States as a whole. To invoke Rule 4(k)(2), a plaintiff must establish that the court's exercise of jurisdiction would be "consistent with the United States Constitution and laws." Fed. R. Civ. P. 4(k)(2); *see also Base Metal Trading, Ltd. v. OJSC "Novokuznetsky Aluminum Factory"*, 283 F.3d 208, 215 (4th Cir. 2002).

We conclude that Rule 4(k)(2) does not justify the exercise of personal jurisdiction over the four banks because exercising jurisdiction over them would not, in the circumstances here, be "consistent with the United States Constitution and laws." Fed. R. Civ. P. 4(k)(2). As we have already noted, subjecting these banks to the "coercive power of a court" in the United States, in the absence of minimum contacts, would constitute a violation of the Due Process Clause. *Saudi v. Northrop Grumman Corp.*, 427 F.3d 271, 275 (4th Cir. 2005).

For the reasons given, the district court's orders dismissing the complaint against the four banks for lack of personal jurisdiction are

AFFIRMED.*

*Although the plaintiffs also claim that the district court abused its discretion in denying them jurisdictional discovery, they only mention the issue in a footnote and do not present argument on the point, thus forfeiting the issue. *See Wahi v. Charleston Area Med. Ctr., Inc.*, 562 F.3d 599, 607 (4th Cir. 2009). In any event, it would appear that the district court did not abuse its discretion in the circumstances of this case. The district court properly recognized the weaknesses of the plaintiffs' arguments for personal jurisdiction and determined that the cost of jurisdictional

discovery would not be justified. This is an appropriate exercise of discretion. *See Rich v. KIS Cal., Inc.*, 121 F.R.D. 254, 259 (M.D.N.C. 1988) ("[W]here a plaintiff's claim of personal jurisdiction appears to be both attenuated and based on bare allegations in the face of specific denials made by defendants, the Court need not permit even limited discovery confined to issues of personal jurisdiction should it conclude that such discovery will be a fishing expedition") (*cited in Carefirst of Md., Inc. v. Carefirst Pregnancy Ctrs., Inc.*, 334 F.3d 390, 403 (4th Cir. 2003)).