Pace Law Review

Volume 32
Issue 3 *Summer 2012*

Article 1

June 2012

Catch Me if You Can: An Analysis of New Enforcement Measures and Proposed Legislation to Combat the Sale of Counterfeit Products on the Internet

Jeffrey A. Lindenbaum
Collen IP

David Ewen
McCarter & English, LLP

Catch Me if You Can: An Analysis of New Enforcement Measures and Proposed Legislation to Combat the Sale of Counterfeit Products on the Internet

Jeffrey A. Lindenbaum* and David Ewen**

I. Introduction

Like many things, the world of counterfeiting was forever changed by the Internet. The virtually impenetrable shield of online anonymity has created an environment where, for the first time, counterfeiters publicly and brazenly advertise, with impunity, that their products are indeed counterfeit. Rather than focusing on a calculable number of counterfeiters in a finite number of well-known and high-trafficked urban centers (e.g., New York City's Chinatown district), brand owners are now faced with counterfeit websites that number in the thousands and change on a daily, and in some instances hourly, basis. Moreover, because a counterfeiter can, with minimal effort and little financial hardship, quickly replace one disabled website with a new one, the traditional enforcement measures have proven ineffective and cost-prohibitive.

The overwhelming volume of counterfeit activity has left the government and brand owners to explore creative measures to attack this problem from new directions. For most it is simply not practical or economically feasible to address counterfeit websites one at a time. Instead, brand owners must seek solutions whereby a single enforcement effort disrupts multiple counterfeit websites.

This Article will discuss two different approaches presently being employed by brand owners to combat this problem. The first involves commencing a single lawsuit against hundreds of

unidentified owners of counterfeit websites. Because of the difficulty with obtaining accurate contact information for the owners of these websites, courts in several jurisdictions have permitted deviations from the traditional methods of service, allowing a plaintiff to effectuate service through, for example, email and online postings. Because the products on these websites are obviously (and in many instances admittedly) counterfeit, courts have seemingly relaxed earlier practices which mandated a physical inspection of the alleged counterfeit products. Likewise, courts have provided injunctive relief directed towards third parties and have required very little, in terms of the posting of a bond to protect the defendants against an unlawful seizure.

The second approach involves using payment processing companies, such as credit card associations, to exercise leverage over their international banking customers to terminate the counterfeiter's bank accounts. These efforts do not focus on disabling a particular counterfeit website, but rather on disrupting the flow of funds to the counterfeit merchant's account. Brand owners hope that, by disabling a merchant's account, they can interrupt the flow of funds to multiple counterfeit websites operated by the same merchant. The Article will highlight the incentives for the credit card associations' cooperation, including protection of their own brands as well as avoiding risks of contributory liability, and persuading Congress that stricter laws and oversight are unnecessary.

Finally, the Article will analyze recent anti-counterfeiting legislation such as the proposed Stop Online Piracy Act and the Protect IP Act, as well as their predecessor, COICA, and opine whether, and how, these types of bills could assist brand owners with the two types of enforcement efforts outlined above. It will also comment on the strongly voiced objections to the legislation lodged by several online business owners and interest groups.

II. The Mass Domain Lawsuit

A search for the phrase "replica rolex watch" on the Google search engine produces 14,200,000 results.[1] Not surprisingly, the first page of these search results provides links to several websites offering counterfeit Rolex watches. Remarkably, nine pages into the search results, there are just as many counterfeit websites—many appearing to be original and unaffiliated with the results found on the earlier search engine result pages. The same is true for the results found at pages seventeen, twenty-nine, and continuing on through the Google results. Commencing a lawsuit to remove just one of these counterfeit websites would be an exercise in futility. This is what many describe as the unending game of "whack-a-mole:" as soon as one website is challenged, several more pop up in its place. Brand owners cannot justify the costs and time needed to prosecute an infringement lawsuit, simply to achieve a default judgment against a single defendant, who will never be identified, never satisfy any monetary judgment, and who will replace his counterfeit website with an entirely new site before the ink is even dry on the complaint.

Seeking a creative alternative, several brand owners have pursued another option. Rather than commence a lawsuit against a single defendant (or a single website), brand owners have commenced what this Article refers to as a "mass domain lawsuit." In these lawsuits, the brand owners join, in one action, as many as five hundred or more John Doe defendants,

* Jeffrey A. Lindenbaum is a partner in the New York Intellectual Property law firm, Collen IP. Mr. Lindenbaum graduated from the University at Buffalo School of Law. A personal thanks and dedication to my wife and boys for all their support, inspiration and for sacrificing quality "Daddy Time" for this Article.

** David Ewen is an associate in the IP/IT department of McCarter & English, LLP in Hartford, Connecticut, and formerly an associate at Collen IP. David obtained his B.A., History from Vassar College in 2004, and J.D. from the University of Connecticut School of Law in 2009.

1. GOOGLE, https://www.google.com/#hl=en&sclient=psyab&q=replica+rolex+watch&pbx=1&oq=replica+rolex+watch&aq=f&aqi=g4&aql=&gs_sm=3&gs_upl=3385l3993l3l6177l2l0l2l0l2l0l0l0l0ll2l0&bav=on.2,or.r_gc.r_pw.r_qf.,cf.osb&fp=e08f40f4badaf740&biw=1366&bih=566 (last visited Feb. 26, 2012). (searching "replica Rolex watch" in Google search).

and target hundreds of counterfeit websites.

The response from each counterfeit defendant fully meets expectations: each of the defendants, without making an appearance, or revealing their identity, has defaulted.[2] The brand owners, through these lawsuits, have taken advantage of the expedited default proceedings to quickly disable mass quantities of counterfeit websites, and interrupt the flow of funds to these sites. With relatively minimum investment, brand owners can make a noticeable impact on the volume of existing counterfeit websites, and quickly move on to the next group of sites.

The relief obtained from these lawsuits is in many respects consistent with traditional counterfeit lawsuits. However, because of the special circumstances that arise from the pursuit of large quantities of quickly-shifting, online counterfeit websites, the courts have endorsed some remedies not typically seen in traditional counterfeit actions. This Section will look at six of the mass domain lawsuits that were filed over the past two years and analyze the similarities and differences between these actions and more traditional counterfeit lawsuits. In the end, it will consider whether the mass domain lawsuit is a successful tool for attacking the "whack-a-mole" problem.

A. *Recent Examples of Mass Domain Lawsuits*

1. Chanel in the Western District of Tennessee

New York-based Chanel, Inc. brought the first of these lawsuits on September 20, 2010, in the United States District Court for the Western District of Tennessee.[3] The complaint, which was filed under seal, named five hundred John Does, and listed 172 defendant domain names.[4] Chanel, owner of the brands CHANEL and the interlocking "CC's" asserted claims for trademark infringement and counterfeiting, false

2. Except for a very small number of defendants who were voluntarily dismissed by the brand owners.

3. Complaint at 1, Chanel, Inc. v. Does 1-172, No. 2:10-cv-2684-STA-dkv (W.D. Tenn. Sept. 20, 2010).

4. *Id.*

designation of origin, cyberpiracy and unfair competition.[5]

The court granted Chanel's *ex parte* motion for a temporary restraining order.[6] The court's order included injunctive relief typical for a trademark counterfeiting action, such as enjoining defendants from manufacturing, importing, promoting, or selling any products bearing the Chanel trademarks, and destroying evidence related to the alleged infringement.[7] But it also granted extraordinary relief, particularly given the very little evidentiary support for each individual website. First, the order states:

> The top-level domain (TLD) Registry for the Subject Domain Names . . . shall change the Registrar of record for the Subject Domain Names to the United States based Registrar GoDaddy.com, Inc. where they will be placed in a holding account in trust for the Court. . . . Additionally, GoDaddy.com, Inc. shall immediately update the Domain Name System ("DNS") data it maintains for the Subject Domain Names, which links the domain names . . . which will cause the domain names to resolve to the website where a copy of the . . . documents on file in this action are displayed. Alternatively, Go Daddy.com, Inc. may institute a domain name forwarding which will automatically redirect any visitor to the Subject Domain Names to the following Uniform Resource Locator ("URL") http://servingnotice.com/oft/ index.html whereon a copy of the . . . file in this action shall be displayed.[8]

The order was not limited to just the domain names listed in the complaint, but also provided that should Chanel, during the pendency of this action, discover additional infringing domain names, these too may be added to the restraining

5. *Id.* at 4:10-14.

6. Order Granting Ex Parte Application for Entry of Temporary Restraining Order at 6, Chanel, Inc. v. Does 1-172, No. 2:10-cv-2684-BBD-dkv (W.D. Tenn. Nov. 4, 2010).

7. *Id.*

8. *Id.* at 7-8:5.

order.[9]

Another distinctive element of this order was its authorization of service via email and by posting the relevant papers on a website:

> Plaintiff shall serve a copy of the *Ex Parte* Application and this Order and all other pleadings and documents on file in this action on Defendants by posting a copy of the *Ex Parte* Application and this Order on the website located at http://servingnotice.com/oft/index.html within forty-eight (48) [hours] of the Subject Domain Names being transferred to the Go Daddy holding account and such notice shall so given shall be deemed good and sufficient service thereof. Plaintiff shall thereafter further provide notice of these proceedings and copies of the documents on file in this matter to Defendants using all email addresses identified in the registration data for each of the Subject Domain Names.[10]

Finally, the court's order mandated that Chanel post a bond in the amount of twenty thousand dollars "prior to requesting the Registries to transfer control of the Subject Domain Names."[11] The order also directed that the file remain sealed until the subject domain names were transferred to the court's control.[12]

Fifteen days later, the court converted the temporary restraining order ("TRO") into a preliminary injunction, adopting the same provisions of the TRO, and unsealed the court file.[13] The preliminary injunction directed that Chanel's

9. *Id.* at 8:8 ("This Temporary Restraining Order shall apply to the Subject Domain Names and any other domain names properly brought to the Court's attention and verified by sworn affidavit to be used by Defendants for the purpose of counterfeiting the Chanel Marks at issue in this action and/or unfairly competing with Chanel in connection with search engine results pages.").

10. *Id.* at 9:11.

11. *Id.* at 8:9.

12. *Id.* at 10:12.

13. Order Granting Application for Preliminary Injunction, Chanel, Inc. v. Does 1-172, No. 2:10-cv-2684-BBD-dkv (W.D. Tenn. Nov. 15, 2010).

twenty-thousand-dollar bond be maintained.[14]

2. Chanel in the District of Nevada (Las Vegas)

Exactly one year after commencing its action in Tennessee, Chanel, on September 20, 2011, brought a second lawsuit in the United States District Court for the District of Nevada.[15] The caption of this action identified the defendants as John Does 1-1000,[16] and the complaint specifically disclosed 399 defendant-domain names.[17] The language of the complaint, motion papers, and resulting temporary restraining order and preliminary injunction tracked those of the earlier-filed Tennessee action.

3. Tiffany in the District of Nevada (Las Vegas)

On April 18, 2011, New Jersey-based Tiffany (NJ), LLC, known for its manufacture of luxury goods, including jewelry, brought suit in the United States District Court for the District of Nevada.[18] The defendants were identified as John Does 1-1000, and the pleading listed 223 defendant-domain names.[19] Tiffany brought claims for trademark counterfeiting and infringement, cyberpiracy, and unfair competition, all pertaining to sixteen registered trademarks, most notably its TIFFANY and TIFFANY & CO. marks.[20]

The relief granted by the court closely followed that obtained by Chanel only a few months earlier in this same court. As with Chanel, Tiffany was required to post a bond of

14. *Id.* at 11:9.

15. Complaint, Chanel, Inc. v. The P'ships & Unincorporated Ass'ns. Identified on Sch. "A", No. 2:11-cv-01508-KJD-PAL (D. Nev. Sept. 20, 2011).

16. *Id.*

17. *Id.*

18. Complaint, Tiffany (NJ), LLC v. The P'ships & Unincorporated Ass'ns. Identified on Sch. "A", No. 2:11-cv-00590-LDG-CWH (D. Nev. Apr. 18, 2011).

19. Order Granting Plaintiff's Ex Parte Application for Entry of Temporary Restraining Order at 10-14, Tiffany (NJ), LLC. v. The P'ships & Unincorporated Ass'ns. Identified on Sch. "A", No. 2:11-cv-00590-LDG-CWH (D. Nev. May 11, 2011).

20. *Id.* at 2-3.

twenty thousand dollars, and was authorized to serve the defendants via email, and by posting the relevant court-filed papers on http://servingnotice.com/off/index.html.[21]

4. Philip Morris in the Southern District of Florida

Philip Morris USA, Inc., a company organized under the laws of, and residing in, Virginia, filed suit in the United States District Court for the Southern District of Florida on November 9, 2011, against defendants Zhilin Jiang, Haidong Huang, Andy Ling a/k/a Andyling, and Does 1-10.[22] The complaint identified fifty-eight defendant-websites.[23] Philip Morris brought claims for trademark counterfeiting and infringement, false designation of origin, and cybersquatting, relating to its MARLBORO mark and its Marlboro packaging design mark.[24]

Similar to the *Chanel* and *Tiffany* matters, Philip Morris was permitted to serve the defendants and provide notice via email and posting a copy of the pleadings at http://servingnotice.com/jiang/index.html.[25] Philip Morris secured the same preliminary relief as Chanel and Tiffany, including transfer of the subject domain names to the court's custody.[26] Notably, the Southern District of Florida also directed non-party Western Union[27] to divert and hold all money transfers to the named defendants, and to provide Philip Morris with records of any money transfers that have been paid to the named defendants. The court's preliminary injunction stated:

21. *Id.* at 8:11,13.

22. Complaint, Philip Morris USA Inc. v. Jiang, No. 1:11-cv-24049-KMM (S.D. Fla. Nov. 9, 2011).

23. *Id.* at 17-18.

24. *Id.* at 4:9-12.

25. Order Granting Ex Parte Application for Alternate Serv. at 3, Philip Morris USA Inc. v. Jiang, No. 1:11-cv-24049-KMM (S.D. Fla. Dec. 6, 2011).

26. Order Granting Application for Entry of Preliminary Injunction, Philip Morris USA Inc. v. Jiang, No. 1:11-CV-24049-KMM (S.D. Fla. Dec. 12, 2011), *available at* http://servingnotice.com/jiang/026%20-%20Order%20Granting%20PI.pdf.

27. *Id.* at 10 n.4 (noting that the preliminary injunction order states that Western Union is licensed to do business in the State of Florida, and is therefore subject to personal jurisdiction in this court).

> Western Union Financial Services, Inc. ("Western Union") shall divert and/or continue diverting all money transfers sent by United States consumers to: (1) Zhilin Jiang in Putian, China . . . (2) Haidong Huang in Putian, China . . . and (3) Haidon Huang . . . and continue to hold such transfers until it receives further direction from the Court.[28]

Although the *Philip Morris* case included considerably fewer domain names and defendants than other lawsuits discussed in this Article, the Southern District of Florida required a noticeably larger bond in the amount of one hundred thousand dollars.[29]

5. True Religion in the Southern District of New York

California-based jeans manufacturers, True Religion Apparel, Inc. and Guru Denim, Inc., filed suit on November 15, 2011, against forty-one defendants and identifying fifty-eight domain names (which increased to eighty-six by the time the temporary restraining order was executed).[30] The suit alleged claims for trademark counterfeiting and infringement, cybersquatting, copyright infringement, unfair competition, false designation of origin, design patent infringement, and unlawful deceptive acts and practices,[31] pertaining to the advertising and sale of counterfeit jeans and other products.[32]

The Southern District of New York issued an order that restrained not only the named defendants, but also "any persons acting in concert or participation with them. . . including, without limitation, Internet Service Providers ("ISP")" from using the True Religion trademarks and copyrights.[33] In addition to enjoining the defendants from

28. *Id.* at 10.

29. *Id.* at 11:12.

30. Complaint at 20, True Religion Apparel, Inc. v. Lei, No. 1:11-cv-08242-HB (S.D.N.Y. Nov. 15, 2011).

31. N.Y. GEN. BUS. LAW § 349 (2010).

32. Complaint at 21-27, True Religion Apparel, Inc. v. Lei, No. 1:11-cv-08242-HB (S.D.N.Y. Nov. 15, 2011).

33. Temporary Restraining Order, Order to Disable Certain Web Sites,

further infringing activity, the court ordered:

> [A]ny third party providing services in connection with any Defendant and/or Defendants' websites, including without limitation, ISPs, back-end service providers, affiliate program providers, web designers, and sponsored search engine or ad-word providers, shall immediately temporarily disable service to any and all Defendants' Infringing Web Sites.[34]
>
> [A]ny third party providing services in connection with any Defendant and/or Defendants' Infringing Web Sites, including without limitation, ISPs, back-end service providers, web designers, sponsored search engine or ad-word providers, banks, merchant account providers including PayPal, Inc., third party processors and other payment processing services, shippers, domain name registrars, domain name registries and online third-party selling platforms (collectively 'Third Party Providers') shall within five (5) days after receipt of such notice provide copies of all documents and records in such person or entity's possession or control relating to[Defendants, their websites and financial accounts owned by Defendants].[35]

Further still, the court's order, in broad, sweeping language, directed any entity that receives actual notice of the order to freeze all financial accounts connected to the defendants or their infringing websites:

> [A]ny banks, savings and loan associations, payment processors or other financial institutions, including without limitation, PayPal, Inc., or other merchant account providers, payment providers, or third party

Asset Restraining Order, Expedited Discovery Order and Order to Show Cause for Preliminary Injunction at 9-10, True Religion Apparel, Inc. v. Lei, No. 1:11-cv-8242-HB (S.D.N.Y. Nov. 18, 2011).

34. *Id.* at 15.

35. *Id.* at 10-11.

> processors for any Defendant, any of Defendants' operations, Defendants' Infringing Web Sites or for any other website owned or controlled by Defendants, who receive actual notice of this Order, shall immediately locate all accounts connected to Defendants or Defendants' Infringing Web Sites and that such accounts be temporarily restrained and enjoined from transferring or disposing of any money or other of Defendants' assets . . . .[36]

The court required the plaintiffs to post a bond of only ten thousand dollars, and authorized service via email to the 137 email addresses identified in the complaint.[37]

6. Coach in the Eastern District of Virginia

Following closely after Chanel's success in Tennessee, Coach, Inc., a corporation organized under the laws of the State of Maryland, and headquartered in New York City, filed suit on March 25, 2011, in in the United States District Court for the Eastern District of Virginia (aptly known as the "Rocket Docket"[38]).[39] Unlike the other mass domain lawsuits discussed in this Article, Coach did not bring its action against a series of unidentified John Doe defendants. Instead, Coach commenced an in rem action, under 15 U.S.C. § 1125(d), against the domain names themselves. Coach's complaint was initially against 419 defendant-domain names, and this number was then expanded to 473 domain names upon the filing of Coach's amended complaint on April 1, 2011.[40] The complaint included

36. *Id.* at 14.

37. *Id.* at 12.

38. This title bestowed on the Eastern District of Virginia dates back approximately forty years, when Judge Albert V. Bryan Jr. decided cases were being managed far too slowly, and began ruling on motions during argument, and was said to have tried an entire case in a single afternoon. *See* Jerry Markon, *A Double Dose of Molasses in the Rocket Docket*, WASH. POST, Oct. 3, 2004, at C04, *available at* http://wp-dr.wpni.com/wp-dyn/articles/A3007-2004Oct2.html.

39. Coach, Inc. v. 1941coachoutletstore.com, 1:11cv309 (JCC/JFA), 2012 WL 27918 (E.D. Va. Jan. 5, 2012).

40. Amended Complaint for In Rem Injunctive Relief, Coach, Inc. v.

a claim for in rem injunctive relief, and asserted Coach's registration, for among others, its COACH mark.[41]

As will be discussed below in detail, this case did not follow track with the other lawsuits discussed in this Article, because although preliminary relief and an injunction were sought, the matter was resolved by way of default before the request for preliminary relief was adjudicated by the court.[42] Also noteworthy is that Magistrate Judge John F. Anderson challenged Coach's joinder of seemingly unrelated defendants into a single suit, as well as Coach's request to serve the defendants and provide notice via electronic means.[43]

B. *Relief Obtained in Mass Domain Lawsuits that is Consistent with Traditional Counterfeit Actions*

Much of the relief secured by the plaintiffs in these mass domain lawsuits is quite common in actions involving sales of counterfeit products. To obtain a temporary restraining order and/or a preliminary injunction in an action involving counterfeit products, federal courts look to whether: (1) the movant has a likelihood of success on the merits; (2) the movant will suffer irreparable harm; and (3) the public interest will be served by issuing the injunction.[44]

Once a brand owner demonstrates a likelihood of consumer confusion, most courts presume that the brand owner will suffer irreparable injury should the infringement continue.[45] Moreover, removing counterfeit goods from the marketplace, and protecting consumers from being misled as to the source of the products they are purchasing, has been widely accepted as

1941coachoutletstore.com, No. 11CV00309, 2011 WL 2621985 (E.D. Va. Apr. 1, 2011).

41. *Id.* ¶ 483.

42. *See* Coach, Inc. v. 1941coachoutletstore.com, 1:11cv309 (JCC/JFA), 2012 WL 27918 (E.D. Va. Jan. 5, 2012).

43. *See* Coach, Inc. v. 1941coachoutletstore.com, 2011 U.S. Dist. LEXIS 150693 (E.D. Va. Nov. 25, 2011).

44. *See* Workman v. Bredesen, 486 F.3d 896, 905 (6th Cir. 2007).

45. *See* Lorillard Tobacco Co. v. Amouri's Grand Foods, Inc., 453 F.3d 377, 382 (6th Cir. 2006); Vision Sports, Inc. v. Melville Corp., 888 F.2d 609, 612 n.3 (9th Cir. 2002); Nautilus Group, Inc. v. Icon Health & Fitness, Inc., 372 F.3d 1330, 1334 (Fed. Cir. 2004).

serving the public interest.[46]

In each of the mass domain lawsuits, the plaintiffs easily established: (1) ownership of the trademarks at issue (each was supported by a federal registration); (2) the defendants had used the marks without authorization of the plaintiff; and (3) the defendants' use is likely to cause confusion (the identical mark was applied to goods intentionally designed to look like products manufactured by the plaintiffs).

Accordingly, it comes as no surprise that the brand owners were able to obtain a temporary restraining order without the defendants being afforded notice and an opportunity to respond. According to 15 U.S.C. § 1116(d), which governs civil actions involving counterfeit marks, "the court may, upon ex parte application, grant an order . . . for the seizure of goods and counterfeit marks involved in such violation and the means of making such marks, and records documenting the manufacturer, sale, or receipt of things involved in such violation."[47]

Likewise, the ordered restraint on future manufacturing and promoting any products bearing the counterfeit marks is far from controversial. Mandating a hold on all documents and information relevant to the counterfeit activity is not only consistent with Section 1116(d), but also with the more general principles that require a hold on discoverable information as soon as litigation is commenced or reasonably anticipated.

Moreover, federal courts, in counterfeit actions, have also routinely permitted a hold on any financial assets that can be reasonably associated with the counterfeit activity.[48] In many cases this results in an order "freezing" bank accounts.

46. *See* Ameritech, Inc. v. Am. Info Techs. Corp., 811 F.2d 960, 964 (6th Cir. 1987); Chanel, Inc. v. Eukuk.com, No. 2:11-cv-01508-KJD-PAL, 2012 U.S. Dist. LEXIS 12904 (D. Nev. Jan. 31, 2012); Louis Vuitton Malletier, S.A. v. P'ships & Unincorporated Ass'ns, No. 2:11-cv-00738-PMP-RJJ2012, U.S. Dist. LEXIS 1481 (D. Nev. Jan. 4, 2012).

47. 15 U.S.C. § 1116(d) (West 2011). Ex parte relief is widely accepted as a necessary means to prevent the alleged counterfeiter from concealing evidence of its actions. *See* Century Home Entm't, Inc. v. Laser Beat, Inc., 859 F. Supp. 636, 638 (E.D.N.Y. 1994); Time Warner Entm't Co. v. Does, 876 F. Supp. 407, 410 (E.D.N.Y. 1994).

48. *See, e.g.*, Levi Strauss & Co. v. Sunrise Int'l Trading, Inc., 51 F.3d 982 (11th Cir. 1995); Microsoft Corp. v. U-Top Printing Corp., No. 93-16048, 1995 U.S. App LEXIS 414 (9th Cir. Jan. 9, 1995).

In light of the broad relief which has long been accepted for counterfeit actions, including that which is expressly authorized under 15 U.S.C. § 1116(d), most of what appears in the temporary restraining orders and preliminary injunctions issued in these mass domain lawsuits is consistent with the relief routinely secured in more traditional, "brick and mortar" counterfeit lawsuits.

C. *Notable Differences Between Relief in Mass Domain Lawsuits and Traditional Counterfeit Actions*

While much of the relief obtained in these mass domain lawsuits runs parallel to that seen in more traditional counterfeit actions, there are several notable departures. Arguably, these departures reflect the courts' endorsement of brand owner's efforts to stretch controlling laws and precedent to overcome the latest hurdles created by the explosion of counterfeit websites. This Section will examine five prominent departures, namely: (1) permitting service and publication by email and on a website; (2) joining of seemingly unrelated defendants in a single lawsuit; (3) lowering the threshold of evidentiary support required to establish that the accused goods are counterfeit; (4) compelling third parties, such as financial institutions and registrars, to take action; and (5) setting a bond amount that represents very little security when considered in connection with the large number of potential defendants impacted by the court's order.

1. Service by Email and Electronic Notice

In the mass domain lawsuits the defendants reside, almost exclusively, outside of the United States—the vast majority being located in China. Accordingly, service for a federal lawsuit is governed by Federal Rule of Civil Procedure 4(f).[49] Rule 4(f) prescribes that a person not within any judicial district of the United States may be served "by any internationally agreed means of service that is reasonably

49. FED. R. CIV. P. 4(f); *see also* FED. R. CIV. P. 4(h)(2) (a foreign corporation may be served "in any manner prescribed by Rule 4(f)").

calculated to give notice, such as those authorized by the Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents."[50] Service under the Hague Convention is a lengthy and costly procedure, which often requires translation and hand delivery of the documents.[51]

Typically, a defendant located in a foreign country that is a member of the Hague Convention (e.g., China), must be served in accordance with the Convention's rules.[52] However, because counterfeit website owners routinely provide fictitious contact information and addresses, the service requirements under the Hague Convention do not apply.[53] Thus, while in most instances concealing the location of a potential defendant makes enforcement more difficult, the website owners have actually helped ease the burden on brand owners.

Since the Hague Convention does not apply in those instances where the defendant has concealed its location, a brand owner may serve the complaint in accordance with Federal Rule 4(f), which provides, in part, that a foreign party may be served by:

> delivering a copy of the summons and of the complaint to the individual personally; or . . . using any form of mail that the clerk addresses and sends to the individual and that requires a

50. FED. R. CIV. P. 4(f)(1).

51. *See* Int'l Soc. for Krishna Consciousness, Inc. v. Lee, 105 F.R.D. 435, 450 (S.D.N.Y. 1984) (citing Pain v. United Techs. Corp., 637 F.2d 775, 788 (D.D.C. 1980)) ("[A] number of courts have observed, the Hague Convention machinery is quite slow and costly even when the foreign government agrees to cooperate.").

52. FED. R. CIV. P. 4(f)(1).

53. Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters, art. 1, Nov. 15, 1965, 20 U.S.T. 361, T.I.A.S. No. 6638, *available at* http://www.hcch.net/upload/conventions/txt14en.pdf ("This Convention shall not apply where the address of the person to be served with the document is not known."); *see* China, People's Republic of, HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW, http://www.hcch.net/index_en.php?act=states.details&sid=30 (The People's Republic of China became a member state of the Hague Convention in 1987); *see also* Gucci Am., Inc. v. Huoqing, No. C-09-05969 JCS, 2011 U.S. Dist. LEXIS 783, at *7 (N.D. Cal. Jan. 5, 2011) (defendant "operates anonymously via the Internet using false physical address information in order to conceal his location and avoid liability for his unlawful conduct.").

> signed receipt; or by other means not prohibited by international agreement, as the court orders.[54]

Service by email was very rare until the Ninth Circuit's decision in *Rio Properties, Inc. v. Rio International Interlink*.[55] In *Rio*, the Ninth Circuit granted the plaintiff's motion under Federal Rule 4(f)(3) to serve the foreign defendant by email.[56] In permitting this deviation, the court first rejected defendant's argument that service by email under Rule 4(f)(3) should only be a last resort, and that there was some hierarchy that must be followed before a party may rely on Rule 4(f)(3).[57] The court concluded that "service of process under Rule 4(f)(3) is neither a 'last resort' nor 'extraordinary relief.' It is merely one means among several which enables service of process on an international defendant."[58]

In deciding whether to permit service of process by email the court held that:

> Even if facially permitted by Rule 4(f)(3), a method of service of process must also comport with constitutional notions of due process. To meet this requirement, the method of service crafted by the district court must be "reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections."[59]

The *Rio* court went on to find that

> [t]o be sure, the Constitution does not require any particular means of service of process, only

54. FED. R. CIV. P. 4(f)(2)-(3).

55. Rio Properties, Inc. v. Rio Int'l Interlink, 284 F.3d 1007, 1014-15 (9th Cir. 2007); *see also* Kevin W. Lewis, *E-Service: Ensuring the Integrity of International E-Mail Service of Process*, 13 ROGER WILLIAMS U. L. REV. 285 (2008); Ronald J. Hedges, Kenneth N. Rashbaum & Adam C. Losey, *Electronic Service of Process at Home and Abroad: Allowing Domestic Electronic Service of Process in the Federal Courts*, 4 FED. CTS. L. REV. 56 (2009).

56. *Rio Properties*, 284 F.3d at 1014-19.

57. *Id.* at 1015-16.

58. *Id.* at 1015 (citations omitted).

59. *Id.* at 1016-1017 (quoting Mullane v. Cent. Hanover Bank & Trust Co., 339 U.S. 306, 314 (1950)).

> that the method selected be reasonably calculated to provide notice and an opportunity to respond. In proper circumstances, this broad constitutional principle unshackles the federal courts from anachronistic methods of service and permits them entry into the technological renaissance.[60]

In *Rio*, the court concluded that service by email was not only proper, but was likely the best means to reach the defendant who "structured its business such that it could be contacted *only* via its email address."[61] Since *Rio*, many other federal courts have permitted service by email using *Rio's* guiding principle that service by email may be appropriate when it proves to be a reliable method to provide the party notice and an opportunity to respond.[62]

In the case of the mass domain lawsuits (including several of those highlighted in this article), most courts have not hesitated to permit service by email. The circumstances presented by the mass domain lawsuits fit squarely within the *Rio* framework for when service by email is proper. First, in the vast majority of these cases, the counterfeit website owners are located outside of the country. Second, because the website owners provide a fictitious address, service under the Hague convention does not apply.[63] Third, in most instances the business of the counterfeit website owners is operated exclusively through the Internet, and email is the most reliable means to successfully reach each defendant.[64] Finally, the courts can take comfort knowing that, at least in the cases discussed in this article, defendants will also receive notice when attempting to visit their own websites, since their

60. *Id.* at 1017 (citations omitted).

61. *Id.* at 1018.

62. *See, e.g.*, Gurung v. Malhotra, No. 10 Civ. 5086 (VM), 2011 U.S. Dist. LEXIS 136578, at *14 (S.D.N.Y. Nov. 22, 2011); *see also* RPost Holdings, Inc. v. Kagan, No. 2:11-cv-238-JRG, 2012 U.S. Dist. LEXIS 7566, at *5 (E.D. Tex. Jan. 23, 2012); *see also* Portal Live, LLC v. Choukron, No.: 11-60203-Civ-Cohn/Seltzer, 2011 U.S. Dist. LEXIS 98623, at *4 (S.D. Fla. Sept. 1, 2011).

63. Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters, *supra* note 53, at art. 1.

64. *See, e.g.*, *Rio Properties*, 284 F.3d at 1018.

domains are re-directed to a page that posts the court file.[65]

One notable exception to the ease in which brand owners have secured permission to serve the pleadings via email, has been the *Coach* case brought in the Eastern District of Virginia. On April 29, 2011, Magistrate Judge John F. Anderson conducted a hearing in which he raised concern about Coach's one-size-fits-all approach to the hundreds of defendants.[66] In particular, Judge Anderson expressed doubt that *all* of the postal addresses associated with the domains were fictitious.[67] Coach relied on the fact that prior to filing suit it had sent cease and desist letters to each of the defendants at their addresses of record, but had not received a single response.[68] Coach concluded that the addresses must be fictitious, never addressing the possibility that some letters were received, but simply ignored. In the end, Judge Anderson ordered that service be provided by postal mail and email.[69]

The mass domain lawsuit brought by Coach in the Eastern District of Virginia rasises another issue regarding notice to a defendant. In that case, Coach brought an *in rem* action under 15 U.S.C. § 1125(d)(2), not against any person or entity, but against the domain names themselves.[70] As such, Coach was also required to publish "notice of the action as the court may direct promptly after filing the action."[71] Coach moved the Court to permit publication via electronic means. Judge Anderson rejected this request as well, but required as an alternative only that Coach publish the notice once in the *Legal Times*.[72]

65. *See, e.g.*, Complaint for Damages and Injunctive Relief, Philip Morris USA, Inc. v. Jiang, Case No. 11-CV-24049-KMM (S.D. Fla. Nov. 9, 2011), *available at* http://servingnotice.com/jiang/index.html; *see also* Complaint for Injunctive Relief, Tiffany (NJ), LLC v. The P'ships & Unincorporated Ass'ns. Identified on Sch. "A", Case No.2:11-cv-00590-LDG-GWF (D.C. Nev. Apr. 18, 2011), *available at* http://servingnotice.com/off/index.html (each court filing is available to the defendants, and the public, in .pdf format).

66. Coach, Inc. v. 1941coachoutletstore.com, No. 1:11cv0309 (JCC/JFA), 2011 U.S. Dist. LEXIS 150693, at *25-26 (E.D. Va. Nov. 25, 2011).

67. *Id.* at *24-25 (emphasis added).

68. *Id.* at *31.

69. *Id.* at *34.

70. *Id.* at *2.

71. 15 U.S.C. § 1125(d)(2)(A)(ii)(II)(bb) (West 2011).

72. Transcript of Hearing at 15, Coach, Inc. v. 1941couchoutletstore.com,

Although Magistrate Anderson's ruling is wholly consistent with traditional methods of providing notice in this country, one must question the practical value of publication in the *Legal Times* for an operator of a counterfeit website that resides, for example, in China. Perhaps recognizing this point, Judge Anderson highlights that because this is an *in rem* action, the notice requirement is not just for the defendant, but for any third party who may have a claim to the property.[73] However, even Judge Anderson acknowledges that this elevates form over function, noting that "[t]his is the fiction we deal with in an *in rem* case."[74]

2. Joinder of Unrelated Defendants

In the mass domain lawsuits, brand owners have joined together in a single suit as many as several hundred different defendants. In some instances, after initially moving against dozens of defendants, brand owners have supplemented their pleadings by submitting several new lists of infringing defendants.[75] To date, no defendant in these mass domain lawsuits has challenged the propriety of joining hundreds of seemingly unrelated defendants; rather almost every defendant has defaulted without making an appearance. The very few defendants that may have made some form of an appearance presumably settled with the brand owners immediately, as it seems the parties quietly stipulated to their dismissal before any responsive papers were filed with the courts.[76]

The issue of joinder, however, was raised by one court. In the *Coach* case, Magistrate Anderson *sua sponte* challenged the propriety of joining numerous defendants into a single suit

No. 1:11-cv-00309-JCC –JFA (E.D. Va. Apr. 29, 2011).

73. *Id.* at 14.

74. *Id.*

75. *See* Memorandum of Points and Auths. in Support of Plaintiff's Second Ex Parte Application for Entry of Temporary Restraining Order and Preliminary Injunction at 18, Chanel v. The P'ships & Unincorporated Ass'ns. Identified on Sch. "A", No. 2:11-CV-01508-KJD-PAL (D. Nev. Nov. 9, 2011).

76. *See, e.g.*, Complaint, Chanel, Inc. v. The P'ships & Unincorporated Ass'ns. Identified on Sch. "A" at 9, No. 2:11-cv-01508-KJD-PAL (D. Nev. Sept. 20, 2011).

where there was no evidence that the defendants were related or associated with one another.[77]

Federal Rule 20(a)(2) states that persons may be joined in one action as defendants if "(A) any right to relief is asserted against them jointly, severally, or in the alternative with respect to or arising out of the same transaction, occurrence, or series of transactions or occurrences; and (B) any question of law or fact common to all defendants will arise in the action."[78] Magistrate Anderson explained that to "satisfy the transaction or occurrence test under *Rule 20(a)(2)*, there must be a logical relationship between the events giving rise to the cause of action against each defendant."[79] Rule 20 "should be construed in light of its purpose, 'to promote trial convenience and expedite the final determination of disputes, thereby preventing multiple lawsuits.'"[80]

The Magistrate's report and recommendation concluded that, but for eleven of the asserted domain names that had a common postal and email address, the remaining 359 domain names asserted in this lawsuit should not have been joined in one action and should be severed.[81] He found that "the evidence presented is insufficient to establish that Coach's claims against *all* defendant domain names are related, that they arise from the same transaction or occurrence, or that there is any joint action among *all* the defendant domain names that warrants relief under the ACPA in a single action."[82] For 11 of the domain names, Magistrate Anderson did find that Coach had satisfied the requirements of Rule 20(a)(2), as it appeared these 11 domain names were registered by the same entity, at the same postal address and 10 of them share the same email address.[83]

Following a timely submitted Objection by Coach, Magistrate Anderson's report and recommendation, pursuant

77. Coach, Inc. v. 1941coachoutletstore.com, No. 1:11cv0309 (JCC/JFA), 2011 U.S. Dist. LEXIS 150693, at *25-26 (E.D. Va. Nov. 25, 2011).

78. FED. R. CIV. P. 20(a)(2).

79. *Coach, Inc.*, 2011 U.S. Dist. LEXIS 150693, at *13 (emphasis added).

80. *Id.* at *14-15 (quoting Saval v. BL Ltd., 710 F.2d 1027, 1031 (4th Cir. 1983)).

81. *Id.* at *43-46.

82. *Id.* at *25.

83. *Id.* at *26-27.

to 28 U.S.C. § 636 and Fed. R. Civ. P. 72, was then reviewed *de novo* by District Court Judge James C. Cacheris.[84] Judge Cacheris ultimately rejected Magistrate Anderson's conclusion that all but eleven of the defendant domain names must be severed from this action.[85] However, Judge Cacheris reached this conclusion without determining whether Coach's allegations comply with the joinder requirements of Rule 20(a)(2).[86] Instead, the court concluded that "it must disregard any potential defects related to joinder, as they do not affect any party's substantial rights, and the Court's correction of those defects under *Rule 21* would not be on just terms."[87] The Court's ruling was based on the fact that each of the defendants in this action was in default: "each Domain Name Defendant is individually subject to default. And, 'there is no prejudice to any defaulting defendant, whose liability may be established upon default irrespective of the presence of any other defendant.'"[88]

Taking a very practical approach, Judge Cacheris avoids determining whether Rule 20 would preclude joinder, recognizing that since each defendant is in default, they suffer no prejudice by having the default entered against them jointly along with hundreds of other unrelated defendants. Practically, the very real prejudice suffered by each defendant is that, but for being able to join hundreds of defendants into a single lawsuit, Coach would almost certainly not have expended the resources to sue each defendant separately. In other words each defendant was likely sued only because joining several hundred defendants in a single lawsuit made it possible (and not cost-prohibitive) to commence the action. This is not likely the type of prejudice a Court would consider because Rules regarding joinder do not create a substantive right not to be sued. Instead, the guiding principle that "*Rule 20* should be

84. Coach, Inc. v. 1941coachoutletstore.com, No. 1:11cv309 (JCC/JFA), 2012 U.S. Dist. LEXIS 1311 (E.D. Va. Jan. 5, 2012).

85. *Id.* at *14.

86. *Id.* at *12-13 (although he does not resolve the merits of the joinder question, notably, he identifies no error in Magistrate Anderson's interpretation of Rule 20(a)(2)).

87. *Id.* at *13.

88. *Id.* at *12-13 (quoting Lyons P'ship, L.P. v. D&L Amusement & Entm't, 702 F. Supp. 2d 104, 112 (E.D.N.Y. 2010)).

construed in light of its purpose 'to promote trial convenience and expedite the final determination of disputes, thereby preventing multiple lawsuits,'" seems to fit squarely with the practical justice rendered by Judge Cacheris.[89]

Had Judge Cacheris not rejected Magistrate Anderson's recommendation, this case could have very well meant the end to the mass domain name lawsuit. But, until the joinder issue is raised by a non-defaulting defendant the mass domain suit will remain an available tool for brand owners to attack counterfeit websites.[90]

3. Lower Threshold of Evidentiary Support to Establish Goods are Counterfeit

Another way that the mass domain lawsuits are distinct from the traditional counterfeit seizure actions is that the courts appear to accept a lower threshold of proof to support the brand owner's allegation that the goods are indeed counterfeit. Under the Counterfeit Statute, a party may obtain an order of seizure with regard to counterfeit activity "based on an affidavit or the verified complaint establishing facts sufficient to support the findings of fact and conclusions of law required for such order."[91] In the traditional counterfeit context, a brand owner would typically satisfy this requirement by hiring an investigator, who would make a purchase (or several purchases) of the alleged counterfeit goods. The goods would then be physically inspected by a corporate representative who is familiar with the company's manufacturing process and use of its brands. Upon finding such goods to be counterfeit, the representative would prepare

89. Coach, Inc. v. 1941coachoutletstore.com, No. 1:11cv0309 (JCC/JFA), 2011 U.S. Dist. LEXIS 150693, at *14-15 (E.D. Va. Nov. 25, 2011) (quoting Saval v. BL Ltd., 710 F.2d 1027, 1031 (4th Cir. 1983)).

90. Although very unlikely to occur in the counterfeit context (particularly given there would be no public interest served), Congress has recently enacted similar laws with regard to patents. *See* 35 U.S.C. § 299 (West 2011) (recent amendments to the Patent Act under The America Invents Act mandating that a "patent troll" establish a closer relationship among defendants before joining them in a single suit for patent infringement).

91. 15 U.S.C. § 1116(d)(3)(A) (2008).

an affidavit, pursuant to §1116(d)(3), attesting to the differences between the brand owner's genuine products, and the counterfeit products.

In the mass domain lawsuits several of these steps have been skipped. In these cases, the brand owners have joined in one lawsuit as many as several hundred different defendants accused of selling counterfeit products. The costs alone for purchasing a sample product from each defendant's website would likely make it cost-prohibitive, or at least highly inefficient to pursue these types of suits. For example, in the *Chanel* case in the Western District of Tennessee, the Complaint identifies 172 defendant domain names.[92] The price of the counterfeit goods at each of these sites ranges from around $50 – $450, with the average price appearing in the range of approximately $150.[93] In addition to the very time-consuming process of coordinating a purchase from each of these locations, the costs for just these purchases alone, would be approximately $30,000 (not including the fees for an investigator to perform the test purchases).

Instead, brand owners have taken a different approach. In many cases, the brand owners have made only a select number of actual purchases. For example, Chanel's Manager of Brand Protection and Enforcement submitted a declaration which indicated that Chanel's independent investigator purchased counterfeit products from only ten of the 172 defendant domains that were joined in the lawsuit.[94] Chanel bolstered this limited investigation by having its internal Manager analyze and assess the content and images displayed on the remaining 162 defendant websites.[95] Based solely on this

92. Complaint, Chanel, Inc. v. Does 1-172, No. 2:10-cv-2684-STA-dkv (W.D. Tenn. Sept. 20, 2010).

93. Aff. of Pilar Toro in Support of Plaintiff's Ex Parte Application for Entry of Temporary Restraining Order and Preliminary Injunction at Ex. 1, Chanel Inc. v. Does 1-172, No. 2:10-cv-02684-BBD-dkv (W.D. Tenn. Sept. 20, 2010), *available at* http://servingnotice.com/oft/20%20-%20dec%20of%20toro.pdf.

94. Declaration of Brandon Scott in Support of Plaintiff's Ex Parte Application for Entry of Temporary Restraining Order and Preliminary Injunction and Order Temporarily Sealing the File ¶ 4, Chanel Inc. v. Does 1-172, No. 2:10-cv-02684-BBD-dkv (W.D. Tenn. Sept. 20, 2010).

95. Declaration of Brandon Scott in Support of Plaintiff's Ex Parte Application for Entry of Temporary Restraining Order and Preliminary

review, the Manager concluded the websites were offering counterfeit products. The Manager affirmed the products were counterfeit based on his "visual inspection of the products, the pricing of the Chanel branded products listed, which are far below the prices of similar genuine Chanel products, and because I personally know Chanel does not conduct business with Defendants or their websites nor do they have the right or authority to use the Chanel Marks for any purpose."[96]

In a more traditional counterfeit context this declaration would be glaringly insufficient to establish that the goods being sold are indeed counterfeit. For example, the fact that Chanel does not authorize the defendant to sell the products, or that the products are listed below Chanel's retail prices, does not take into account that the goods could be gray market (i.e., genuine goods manufactured by the brand owner, but sold through unauthorized channels), or could be goods that are used (second hand) and being resold on the website.

The Manager's visual inspection of the product images is likewise of limited value, because the Manager never possessed or inspected the actual product – only a picture that is posted on the website. In addition to not being able to completely inspect the physical sample from all angles, it fails to take account that the picture posted on the website may not be an actual representation of the product being sold. It takes little imagination to envision that a counterfeit website may post pictures of genuine Chanel products (even images copied from Chanel's own website) to promote its sale of counterfeit products.

A second problem exists insofar as the Manager who inspects the products online states that he goes through the steps to make a purchase, places the items in an online shopping cart, but does not actually complete the transaction.[97] Accordingly, the brand owner cannot verify for the Court that the products are actually being sold on the website.[98] Seeking

Injunction and Order Temporarily Sealing the File ¶¶ 11-13, Chanel Inc. v. Does 1-172, No. 2:10-cv-02684-BBD-dkv (W.D. Tenn. Sept. 20, 2010).

96. *Id.* ¶ 10.

97. *Id.* ¶ 10.

98. Of course, a party may be liable for infringement for merely offering to sell a counterfeit product; however, without an actual sale, it would seem

the extraordinary relief of obtaining an *ex parte* temporary restraining order and asset freeze without actually making a purchase from the defendant and without physically inspecting the product seems contrary to the strict evidentiary thresholds traditionally imposed by courts in evaluating whether an *ex parte* temporary restraining order is appropriate.[99]

However, in the present world of online counterfeit sales, the website owners have solved this problem for the brand owners. In most instances, physical inspection of the product is no longer necessary. This is because the counterfeit activity on the Internet has become so brazen that the counterfeiters no longer conceal the fact that the products they sell are counterfeit. Indeed, as Chanel's Manager explains in his declaration, many of the websites include disclaimers which "expressly acknowledge the Chanel branded goods sold thereon are 'replica.'"[100]

An example of this type of admission can be found at the website located at www.exactwatches.com, where the merchant proudly proclaims:

> Have you always wanted a fake Rolex or a Breitling replica but always thought it was too expensive for your budget or even for your taste? . . . Our fake Rolex watches and Breitling replicas are some of the best to be created by man. Experts say that our replicas are so accurate that they are hard to spot as "knockoffs." This means that purchasing a $120-watch from us will make you look like the wealthiest man on your street, simply because our replicas look so real and authentic.[101]

Accordingly, in instances, such as with the website located at exactwatches.com, a test purchase of the counterfeit products has, in many respects, become redundant. The counterfeiters themselves have already conceded that their

to present a less compelling basis for granting the extraordinary relief of an *ex parte seizure* and asset freeze. *See* 15 U.S.C. § 1116(d)(1)(A).

99. *See In re* Lorillard Tobacco Co., 370 F.3d 982, 989 (9th Cir. 2004).

100. Aff. of Pilar Toro, *supra* note 93, ¶ 10.

101. EXACT WATCHES, http://www.exactwatches.com (last visited March 6, 2012).

websites are only selling counterfeits. But for those instances where a website itself does not expressly admit that the products being sold are counterfeit, a court arguably could have a valid basis to refuse to issue an *ex parte* order of seizure against a defendant website, let alone hundreds of websites, based solely on inspection of images found on the website.

4. Directing Third Parties

The temporary restraining orders and preliminary injunctions issued in the mass domain lawsuits are not directed solely at the defendants. These orders also direct third parties to take certain actions related to the infringing websites.

For example, in the *True Religion* case the Court ordered that all banks, payment processors and financial institutions (including PayPal) shall freeze all financial accounts for the defendants or the defendants' websites.[102] The asset freeze not only enjoined these financial institutions from transferring any funds to the defendants, they also enjoined the institutions from providing any chargebacks or refunds to any consumers who (innocently or otherwise) placed orders for the counterfeit goods.[103]

Likewise, in the *Philip Morris* case, the Southern District of Florida ordered that Western Union shall divert all money transfers sent to the defendants.[104] In doing so, the court noted that Western Union was licensed to do business in the State of Florida, and therefore subject to jurisdiction in that district.[105] The order permitted Western Union to respond to any customer inquiries by advising of the pending lawsuit, and directing the customers to Philip Morris' counsel who was required to provide the customers with a report of the status of their

102. Temporary Restraining Order, Order to Disable Certain Web Sites, Asset Restraining Order, Expedited Discovery Order, and Order to Show Cause for Preliminary Injunction ¶ 11, True Religion Apparel Group, Inc. v. Lei, No. 1:11-cv-08242-HB (S.D.N.Y. Nov. 18, 2011).

103. *Id.*

104. Order Granting Application for Entry of Preliminary Injunction at 10:9, Philip Morris USA, Inc., v. Jiang, No. 1:11-cv-24049-KMM (S.D. Fla. Dec. 12, 2011).

105. *Id.* at 10:9 n.4.

transaction.[106]

Well prior to the institution of these mass domain lawsuits, many courts, particularly in connection with counterfeit actions, have directed financial institutions to freeze a defendant's assets. In *Reebok International v. Marnatech Enterprises,* the Ninth Circuit reasoned that an asset freeze in a counterfeit lawsuit could be supported by Federal Rule 64, 15 U.S.C. §§ 1116 and 1117, and the inherent powers of the Court.[107] The Court ultimately concluded that "[b]ecause the Lanham Act authorizes the district court to grant [plaintiff] an accounting of [defendant's] profits as a form of final equitable relief [under Section 1117], the district court had the inherent power to freeze [defendant's] assets in order to ensure the availability of that final relief."[108] This same reasoning was adopted by the Eleventh Circuit a few years later in *Levi Strauss & Co. v. Sunrise International Trading.*[109]

The redirection of Western Union transactions pertaining to the defendants in the *Philip Morris* case, however, presents a deviation from the traditional counterfeit defendant asset freeze. First, the asset freeze is not limited to just funds that already reside in the defendant's bank account. The order requires Western Union to continue to re-direct any monetary transfers that would otherwise be delivered to the defendants.[110]

Second, in these types of cases, a counterfeit defendant is likely to be operating more than one counterfeit website. This creates the likelihood that, although some of the defendants' websites may be disabled per the courts' TRO, others are likely not included in the order and may continue to operate. These other websites presumably continue to receive monetary transfers through Western Union from consumer purchases from the non-disabled websites. Accordingly, the court's order,

106. *Id.* at 11:11.

107. *See* Reebok Int'l, LTD. v. Marnatech Enters. Inc., 970 F.2d 552, 558-60 (9th Cir. 1992).

108. *Id.*

109. 51 F.3d 982, 987 (11th Cir. 1995).

110. Order Granting Application for Entry of Preliminary Injunction at 10:9-11, Philip Morris USA, Inc., v. Jiang, No. 1:11-CV-24049-KMM (S.D. Fla. Dec. 12, 2011).

which compels redirection of all Western Union transfers to the *defendants*, as opposed to just transactions pertaining to the disabled *websites*, not only impacts assets already held in a defendant's bank account, but also creates a situation whereby, on an ongoing basis, funds from consumer purchases from surviving defendant-operated counterfeit websites are re-directed and held during the pendency of the case. In other words, long after the court issues a TRO, consumers visiting other websites owned by the defendants, may have their funds redirected by Western Union and seized by the court.

In addition, several of the court orders in these mass domain lawsuits require the relevant registries to transfer the domain names to an account with GoDaddy.com, Inc., where they are held in trust for the Court during the pendency of the case, and redirected to a website that displays the pleadings and court filings for the lawsuit.[111]

In a traditional counterfeit lawsuit, the scope of the order of seizure and preliminary injunction is typically limited to confiscation of, and an injunction pertaining to, counterfeit products bearing the moving plaintiff's brands. It is firmly held that "[i]njunctive relief should be narrowly tailored to fit specific legal violations."[112] In the mass domain lawsuits, the courts have directed third parties to disable not only the portions of the infringing websites that pertain to sales of products bearing the brand owner's trademarks, but the defendants' entire websites, including portions of these websites that are dedicated to sales of products that do not use the moving parties' brands (but likely infringe on other, non-party, brands). Applied to the typical "brick and mortar" counterfeit action, this would be the equivalent of directing a landlord to lock a tenant's entire store, without notice, and deposit the key with the court until the conclusion of the lawsuit, even if that tenant sells a variety of products that do not bear the plaintiff's trademark, and are not the subject of

111. Order Granting Ex Parte Application For Entry of Temporary Restraining Order at 7, Chanel, Inc. v. Does 1-172, No. 2:10-CV-2684-BBD-dkv (W.D. Tenn. Nov. 4, 2010).

112. Patsy's Brand, Inc. v. I.O.B. Realty, Inc., 317 F.3d 209, 220 (2d Cir. 2003) (quoting Waldman Pub. Corp. v. Landoll, Inc., 43 F.3d 775, 785 (2d Cir.1994)); *see also* N. Face Apparel Corp. v. TC Fashions, Inc., No. 05 Civ. 9083 (RMB), 2006 U.S. Dist. LEXIS 14226 (S.D.N.Y. Mar. 30, 2006).

the claims asserted in the lawsuit. Such an extreme form of relief would almost certainly garner greater scrutiny in the traditional "brick and mortar" context.

The effectiveness of the domain name transfer is largely dependent on the case file remaining sealed until the transfer is complete. As explained by Chanel in the Tennessee lawsuit:

> [T]he Defendants operate Internet websites which they optimize for the sale of counterfeit Chanel merchandise. The optimization process provides the Defendants with their power to unfairly compete with Chanel by catapulting their illegal websites into search engine results. All of the optimization power which has been built through the illegal use of the Chanel Marks can easily be transferred to a new domain name in a matter of minutes through what is known as a redirect. A redirect is essentially a command which instructs search engines such as Google to transfer or redirect all traffic and the benefits thereof to a new domain name. . . . The only way to avoid the probability of successful redirects to evade an injunction is to secure and disable the domain names in advance of notice to the Defendants or the public.[113]

The redirection of the infringing domains to a website that displays information regarding the pending lawsuit serves several functions. First, as discussed above, it provides a means for serving notice and process on the defendants regarding the seizure of their website and the filings with the Court. Second, perhaps the most obvious, is that it terminates the infringing sales and use of the counterfeit marks (at least at this one particular site), and disrupts the counterfeit defendant's efforts to maintain a prominent presence in search

113. Memorandum of Points and Authorities in Support of Chanel, Inc.'s Ex Parte Application for Entry of Temporary Restraining Order and Preliminary Injunction and Order Temporarily Sealing the File at 28-29, Chanel Inc. v. Does 1-172, No. 2:10-cv-02684-SHM-dkv (W.D. Tenn. Sept. 21, 2010).

engine results for the counterfeit goods. Third, it provides notice to consumers (unsuspecting or otherwise) that the products being offered at these websites (and by inference many others), are unlawful, and that brand owners, and the courts are taking legal measures to enjoin such activity.

The result of these actions should not only be a deterrent against those who knowingly patronize these types of counterfeit websites, but also protection for naïve consumers, who may unknowingly be purchasing counterfeits, or supplying credit card and personal information to a phishing site.

Finally, redirection of the counterfeit websites provides free access to the case file for the general public, including consumer watch groups, so that the arguments presented to the Court, and the relief being granted by the Court, may be closely monitored, and where appropriate, challenged.

5. Setting a Low Bond

To obtain an Order permitting seizure of counterfeit goods, a plaintiff must post a bond.[114] Section 1116(d)(4) states that the "court shall not grant such an application unless the person obtaining an order under this subsection provides the security determined adequate by the court for the payment of such damages as any person may be entitled to recover as a result of a wrongful seizure or wrongful attempted seizure under this subsection."[115] The court has discretion to determine the appropriate amount of a bond posted in connection with a preliminary injunction or temporary restraining order.[116] In setting the amount of a bond, some courts maintain they should "err on the side of caution—that is, toward larger bonds—in light of the need to protect the unrepresented defendant, and to ensure that the defendant will have an effective remedy if he or she is the victim of a wrongful seizure."[117]

114. 15 U.S.C. § 1116(d)(4) (2006); Hoechst Diafoil Co. v. Nan Ya Plastics Corp., 174 F.3d 411, 421 (4th Cir. 1999).

115. 15 U.S.C. § 1116(d)(4)(A) (2006).

116. *Hoechst*, 174 F.3d at 421.

117. Time Warner Entm't Co. v. Does, 876 F. Supp. 407, 411 (E.D.N.Y. 1994) (citing 130 Cong. Rec. H12076 (daily ed. Oct. 10, 1984) (statement of

The potential recovery for a wrongful seizure brought under 15 U.S.C. § 1116(d) is limited to the amount of the bond that is posted by the plaintiff.[118] In the two *Chanel* cases and the *Tiffany* case discussed above, the courts required the plaintiffs to post a bond in the amount of $20,000.[119] In the *True Religion* case, the New York court only required a bond of $10,000.[120] And in the *Philip Morris* case, the court required a bond of $100,000.[121] Given the blatant acts of counterfeiting complained of in each of these lawsuits, the amounts of these bonds, at first glance, seem reasonable. However, the sufficiency of the bonds must be analyzed in light of the huge number of defendants and domains that are joined in the single lawsuit. For example, in the *True Religion* case, an order of seizure was issued with regard to 86 separate defendant domains. Thus, each seized domain is potentially secured by only $116.27. The *Chanel* action in Las Vegas, secured by a $20,000 bond, identifies 399 domains.[122] Here, each domain may be secured by only $50.12.

Naturally, it is extremely unlikely that in a case brought against, for example 399 counterfeit websites, that each would succeed in challenging the seizure, and be entitled to a portion

Rep. McCarthy)) ("Congress noted that the provision of a bond is one of the critical procedural protections designed to ensure that the defendant's rights are adequately protected during the course of an ex parte seizure.").

118. Blau v. YMI Jeanswear, Inc., No. CV 02-09551 FMC (SHSx), 2003 U.S. Dist. LEXIS 27432, at *22 (C.D. Cal. Dec. 31, 2003).

119. Order Granting Application for Preliminary Injunction at 11, Chanel, Inc. v. Does 1-172, No. 2:10-CV-2684-BBD-dkv (W.D. Tenn. Jan. 3, 2011); Order Granting Plaintiff's Ex Parte Application for Entry of Temporary Restraining Order and Preliminary Injunction, Chanel, Inc. v. The P'ships and Unincorporated Ass'ns Identified on Sch. "A", 2:11-CV-1508-KJD-PAL (D. Nev. Sept. 26, 2011); Order Granting Plaintiff's Ex Parte Application for Entry of Temporary Restraining Order, Tiffany v. Does, 2:11-CV-590-LDG-CWH (D. Nev. May 11, 2011).

120. *See* Temporary Restraining Order, Order to Disable Certain Web Sites, Asset Restraining Order, Expedited Discovery Order and Order to Show Cause for Preliminary Injunction at 12, True Religion Apparel, Inc. v. Lei, 1:11-CV-8242-HB (S.D.N.Y. Nov. 18, 2011).

121. *See* Order Granting Application for Entry of Preliminary Injunction at 11, Philip Morris v. Jiang, No. 1:11-CV-24049-KMM (S.D. Fla. Dec. 12, 2011).

122. *See* Complaint for Injunctive Relief, Chanel, Inc. v. The P'ships and Unincorporated Ass'ns Identified on Sch. "A", 2:11-CV-1508-KJD-PAL (D. Nev. Sept. 20, 2012).

of the bond. However, it seems equally unlikely that the courts have fully considered the ramifications should this occur, whereby one of these defendants could be left with a mere $50 as secured damages resulting from an improper seizure of its website.

D. *Evaluating the Effectiveness of the Mass Domain Lawsuit*

To date, the mass domain lawsuits have been effective in achieving their immediate purpose, namely to disable a large number of counterfeit websites and interrupt the flow of funds generated from these sites. Statistically, the ratio of websites disrupted compared to the number of mass domain lawsuits filed is impressive. Notwithstanding its success, it is premature to determine whether the mass domain lawsuit can effectively curtail the expansion of online counterfeit websites.

First, the mass domain lawsuit format has yet to be challenged by any defendant, as all of the defendants in these lawsuits have defaulted (or have been dismissed) without posing any substantive challenge. Some of the potential vulnerabilities of the mass domain lawsuit format were highlighted in the *Coach* case discussed above. However, until a defendant attempts to defend its website, rather than default, it remains to be seen whether this type of lawsuit could ultimately withstand challenge.

Second, although the brand owners' success in disabling a large volume of websites with the filing of just a few lawsuits is remarkable, these efforts may be undermined if the counterfeit website owners can keep pace by creating new sites, or by redirecting old sites, to replace those that were disabled by these lawsuits. Given the incredibly large number of counterfeit websites that already exist, with new sites popping up every day, it is unlikely that the website owners can be out-paced by only the mass domain lawsuits. However, hope remains that a brand owner, through the diligent employment of these mass domain lawsuits, combined with some other aggressive tools, including those discussed in the next section, can, at minimum, eliminate a counterfeiter's incentive to peddle counterfeit products bearing that company's brand.

III. Termination of Counterfeit Merchant Accounts Through Cooperation with Payment Processors

Suing Doe defendants and websites *en masse* has thus far proven an efficient means of pursuing counterfeiters directly. However, trademark law also affords brand owners the potential to recover from secondary infringers who induce infringement or knowingly provide their services to counterfeiters. With internet counterfeiting largely dependent on credit card transactions, brand owners exploring theories of secondary liability are now "following the money." This Part will discuss brand owners' options for holding credit card associations accountable for the acts of counterfeiting transacted through their networks. It will also consider the card associations' incentives and responsibilities for assisting brand owners' efforts to disrupt counterfeiters' businesses.

A. *Understanding Credit Card Transactions*

1. Overview of Payment System

The starting point for a brand owner seeking to hold third-party service providers liable is to identify who are the players, and what are their roles. To understand the applicability of secondary liability in the context of credit card payment processing, it is necessary to distinguish the two primary models for credit card transactions: the Visa/MasterCard model, and the American Express/Discover model. In each model, the card association's (i.e., Visa, American Express) relationships with merchants (here, the counterfeiters) and cardholders differ.

The Visa/MasterCard model is known as a "four-party" system.[123] In a four-party system, a credit card transaction

123. MASTERCARD WORLDWIDE, BENEFITS OF OPEN PAYMENT SYSTEMS AND THE ROLE OF INTERCHANGE (2008), *available at* http://www.mastercard.com/us/company/en/docs/BENEFITS%20OF%20ELECTRONIC%20PAYMENTS%20-%20US%20EDITION.pdf [hereinafter MASTERCARD BENEFITS] ; Visa, Inc., *Visa Transaction*, ABOUT VISA, http://corporate.visa.com/about-visa/our-business/visa-transaction.shtml (last visited Mar. 6, 2012); ANN KJOS, THE MERCHANT-ACQUIRING SIDE OF THE

involves (1) a cardholder; (2) the financial institution that issues the cardholder's credit card; (3) the merchant; and (4) the financial institution that "acquires" the merchant's account.[124] The financial institutions described in (2) and (4) are commonly referred to as "issuing banks" and "acquiring banks," respectively.[125] Though it is referred to as a four-party system, in practice, there are often more than four parties involved in a credit card transaction, as the acquiring banks typically outsource all merchant-acquiring services other than financing.[126]

Moreover, the designation "four-party system" does not count the payment network or card association involved. This omission likely stems from the fact that, until recently, Visa and MasterCard were structured as non-profit, joint ventures owned by the issuing and acquiring banks themselves.[127] In their respective systems, Visa and MasterCard operate the payment network that allows the issuing and acquiring banks using that network to communicate and transmit funds in order to authorize, clear, and settle transactions.[128] In addition to providing a medium for issuing and acquiring banks to communicate, Visa and MasterCard promulgate operating regulations governing use of their payment networks by their client financial institutions and, by imposing duties upon those institutions, merchants.[129] Among other things, these operating

PAYMENT CARD INDUSTRY: STRUCTURE, OPERATIONS, AND CHALLENGES 2 (2007), *available at* http://www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2007/D2007OctoberMerchantAcquiring.pdf (the four-party system is also known as an "open-loop" system, or "bank-centered payment networks").

124. *Visa Transaction*, *supra* note 123.

125. KJOS, *supra* note 123, at 2.

126. Adam J. Levitin, *Priceless? The Competitive Costs of Credit Card Merchant Restraints* (Georgetown Law Faculty Working Papers, Paper No. 22, 2007), *available at* http://scholarship.law.georgetown.edu/fwps_papers/22.

127. *Id.* at 6; United States v. Visa U.S.A., Inc., 344 F.3d 229, 235 (2d Cir. 2003). Before going public, Visa and MasterCard's profits were "held basically as security accounts, to pay merchants in the event a member bank defaults on a payment obligation." *Visa U.S.A., Inc.*, 344 F.3d at 235.

128. *Payment Processing*, MASTERCARD WORLDWIDE, http://www.mastercard.com/us/company/en/whatwedo/payment_processing.html (last visited March 5, 2012).

129. MASTERCARD WORLDWIDE, MASTERCARD RULES, 5-1 to 5-20 (2012), *available at* http://www.mastercard.com/us/merchant/pdf/BM-

regulations are designed to manage risk,[130] monitor merchant activities, and protect the VISA and MASTERCARD brands.[131]

Visa and MasterCard do not directly contract with cardholders or merchants. Rather, it is the issuing and acquiring banks, or often their own agents or third-party contractors, that form direct relationships with the cardholders and merchants.[132] As part of their relationship with cardholders, issuing banks perform functions such as extending credit, issuing billing statements, and collecting payments.[133] On the merchant side, acquiring banks manage merchant accounts, process payments,[134] and provide merchants with a gateway to interface with the payment network and the issuing banks.[135]

2. Anatomy of a Credit Card Transaction

To better understand the four parties' roles, it is helpful to consider the anatomy of a typical credit card transaction. There are three discrete stages in a credit card transaction: authorization, clearing, and settlement. Authorization occurs

Entire_Manual_public.pdf [hereinafter MASTERCARD RULES]; VISA, VISA INTERNATIONAL OPERATING REGULATIONS 400-17 (2012), *available at* http://usa.visa.com/download/merchants/visa-international-operating-regulations-main.pdf.

130. Acquiring banks and issuing banks bear different types of risk. Ramon P. DeGennaro, *Merchant Acquirers and Payment Card Processors: A Look Inside the Black Box*, 91 FED. RES. BANK OF ATLANTA ECON. REV. 27, 34-37 (2006), *available at* http://www.frbatlanta.org/filelegacydocs/erq106_degennaro.pdf. An issuing bank, which extends credit to cardholders, bears the risk of the cardholder defaulting on payment. *Id.* Acquiring banks bear risk with respect to transactions disputed by cardholders, also known as "chargebacks." *Id.* In the case of a chargeback, the acquiring bank indemnifies the issuing bank (who indemnifies the cardholder) for the purchase price; if the merchant has inadequate funds to cover the chargeback, the acquiring bank is left holding the bag. *Id.*

131. MASTERCARD RULES, *supra* note 129, at 4-1 to 4-2; VISA, *supra* note 129, at 104.

132. KJOS, *supra* note 123, at 2-3.

133. DeGennaro, *supra* note 130, at 31.

134. *See id.* Some, often larger, acquirers process payments themselves; others, often smaller, resell the processing services of third parties. *Id.*

135. *Id.*

before any funds are actually transmitted between banks, consisting of the approval or denial of a proposed transaction.[136] During clearing and settlement, funds are transmitted between banks, the cardholder is billed, and bank and network fees are deducted from the amount remitted to the merchant.[137]

A transaction begins with the cardholder swiping her card at a merchant's payment terminal, or submitting her card information through a website. The terminal (or website) transmits the cardholder's information to the acquiring bank. Next, the acquiring bank submits this information into the payment network, which then routes the information to the cardholder's issuing bank. After receiving the card information and querying the cardholder's account, if approved, the issuing bank transmits an authorization through the payment network back to the initiating acquiring bank. The acquiring bank forwards the authorization to the merchant, permitting the transaction to go forward.[138] This ends the authorization stage.

Though at this point the buyer has already left with her goods (or has perhaps received a purchase and delivery confirmation by email), the back-end processes of clearance and settlement continue. To initiate these processes, the merchant must submit its transactions to its acquiring bank to begin clearance and settlement – the point at which funds are deposited into the merchant's account for the purchased goods, and the participating parties make their money. Upon receipt of transaction information, the issuing bank will bill the appropriate cardholder's account with the purchase amount, and remit the purchase amount, less the "interchange fee" prescribed by the card association, through the payment network. As the funds make their way to the acquiring bank, the card association will deduct an "assessment fee" for its own services, and pass on the remainder to the acquiring bank.[139]

136. Visa Inc., Annual Report (Form 10-K), at 7 (Nov. 19, 2010), *available at* http://www.sec.gov/Archives/edgar/data/1403161/000119312510265236/d10k.htm.

137. *Id.*

138. KJOS, *supra* note 123, at 4-5.

139. *Id.* at 20.

Likewise, the acquiring bank deducts a fee of its own, and credits the merchant's account with what remains. Together, the interchange fee retained by the issuing bank, the assessments fee retained by the card association, and acquiring fee retained by the acquiring bank comprise the "merchant discount fee."[140]

3. The Three-Party System

In contrast, American Express and Discover operate under a "three-party system,"[141] or "closed" network.[142] The primary difference from the Visa/MasterCard model is that in the three-party system used by American Express and Discover, "the generally independent functions of issuers, acquirers, and networks that exist in the Visa/MasterCard models are collapsed into one entity."[143] That is, unlike Visa and MasterCard, American Express and Discover not only manage the payment network, but traditionally also play the role of issuing bank and acquiring bank, forming direct contractual relationships with cardholders and merchants to use and accept their payment cards.[144] To the average cardholder, the difference between three- and four-party systems may seem academic. But for purposes of a card association's exposure to contributory liability for merchants' infringements, the distinction may be critical.

B. *Contributory Liability and Payment Processors*

In two prominent cases, brand owners have sought to have card associations, acquiring banks, and/or payment processors answer for the infringements of the merchants they serve. Because they are processing payments, not peddling counterfeit goods themselves, the theories of liability advanced against participants in credit card payment processing center

140. *Id.* at 20-21.

141. MASTERCARD BENEFITS, *supra* note 123, at 3.

142. United States v. Visa U.S.A. Inc., 163 F. Supp. 2d 322, 333 (S.D.N.Y. 1991).

143. KJOS, *supra* note 123, at 3.

144. KJOS, *supra* note 123, at 3; Levitin, *supra* note 126, at 7.

on the doctrines of vicarious and contributory trademark infringement. A vicarious infringer is "one who has an apparent or actual partnership with the infringer or who exercises joint ownership or control over the infringing product."[145] In contrast, contributory liability extends to those who "knowingly cooperate in illegal and tortuous activity."[146] Though plaintiffs have advanced both theories of secondary liability (as well as unsuccessful claims for direct infringement) against participants in credit card payment processing, for purposes of this article, the discussion of card networks' potential liability will be limited to the doctrine of contributory liability.

1. Development of Contributory Liability for Service Providers

The recent extension (and attempted extension) of contributory liability to service providers, and particularly to participants in credit card payment processing, has its roots in the Supreme Court's decision in *Inwood Laboratories, Inc. v. Ives Laboratories., Inc.*[147] *Inwood* involved a dispute between two prescription drug manufacturers. Inwood allegedly sold its generic drug in identically colored capsules as Ives, inducing pharmacists to mislabel Inwood's generic drug with Ives' registered trademark, CYCLOSPASMOL.[148] On this basis, Ives sued Inwood for trademark infringement. The district court denied Ives' request for a preliminary injunction, and in a bench trial, entered judgment for the defendant, Inwood.[149] The Second Circuit reversed, finding Inwood liable for contributory

145. 4 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 25:22 (4th ed. 2011).

146. *Id.* § 25:17.

147. 456 U.S. 844 (1982). *Inwood* was not the Supreme Court's first exposure to secondary liability. For a discussion of pre-*Inwood* contributory liability case law, see Charles W. Adams, *Indirect Infringement from a Tort Law Perspective*, 42 U. RICH. L. REV. 635, 675-77 (2008).

148. 456 U.S. at 850.

149. Ives Labs., Inc. v. Darby Drug Co., 455 F. Supp. 939 (E.D.N.Y. 1978), *aff'd*, 601 F.2d 631 (2d Cir. 1979) (denying preliminary injunction); Ives Labs., Inc. v. Darby Drug Co., 488 F. Supp. 394, 397-98 (E.D.N.Y. 1980) (denying Ives' claim for contributory trademark infringement under Lanham Act § 32), *rev'd*, 638 F.2d 538 (2d Cir. 1981).

trademark infringement.[150]

The Supreme Court then reversed the Second Circuit's decision, finding that the trial court's denial of Ives' contributory infringement claim was not clearly erroneous.[151] However, the Supreme Court confirmed that a manufacturer could be held liable even where it did not "directly control" pharmacists who mislabeled the drug with another's trademark.[152] The Court articulated a two-pronged doctrine of contributory liability, where a manufacturer or distributor could be found contributorily liable if it "intentionally induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement."[153]

A decade later, *Inwood* was applied outside of the manufacturer/distributor and "product" contexts. The United States Courts of Appeals for the Seventh and Ninth Circuit, drawing upon the tort law concept of premises liability, held that operators of flea markets and swap meets could be held contributorily liable for the trademark infringements committed by vendors on their premises.[154] And just a few years thereafter, the Ninth Circuit decided what has become the seminal case in extending *Inwood's* concept of contributory liability to service providers: *Lockheed Martin v. Network Solutions, Inc.*[155]

In *Lockheed*, the defendant was a domain name registrar.[156] The plaintiff, owner of the service mark SKUNK WORKS had notified the defendant of domain name

150. 638 F.2d at 540.

151. 456 U.S. at 858. Because the Second Circuit did not consider Ives' unfair competition claims under § 43(a) and state law, the Supreme Court remanded these issues. *Id.* at 859.

152. *Id.* at 853-54.

153. *Id.* at 854 (citing William R. Warner & Co. v. Eli Lilly & Co., 265 U.S. 526 (1924); Coca-Cola Co. v. Snow Crest Beverages, Inc., 64 F.Supp. 980 (Mass. 1946), *aff'd*, 162 F.2d 280 (1st Cir. 1947), *cert. denied*, 332 U.S. 809 (1947)).

154. Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1149 (7th Cir. 1992) (contributory liability may attach to flea market operator); *accord*, Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 265 (9th Cir. 1996) (swap meet operator).

155. 194 F.3d 980 (9th Cir. 1999).

156. *Id.* at 982.

registrations containing its service mark or confusingly similar variations, demanded that the domains be cancelled, and demanded that the defendant refuse to register any like domains in the future.[157] When the defendant did not comply, the plaintiff sued for contributory infringement, as well as other claims under the Lanham Act.[158]

Because the defendant registrar provided to the third-party infringers a service, rather than a product, the case did not fit neatly within the *Inwood* mold. Building upon the Seventh Circuit's decision in *Hard Rock*, and its own in *Fonovisa*, the Ninth Circuit adapted the second prong of the *Inwood* test to the context of service providers.[159] In determining whether a service provider would be held liable for contributory infringement, the Court looked to "the extent of control exercised by the defendant over the third party's means of infringement."[160] The Court concluded that contributory liability would arise where the service provider exercised "[d]irect control and monitoring of the instrumentality used by a third party to infringe the plaintiff's mark."[161] Ultimately, the defendant's rote translation of domain names into corresponding internet protocol addresses was insufficient to warrant a finding of contributory liability.[162]

2. Application of Contributory Infringement Doctrine to Payment Processors

a. Perfect 10 v. Visa International Service Association

The Ninth Circuit had an opportunity to apply the *Lockheed* standard directly to payment processors and card associations in *Perfect 10, Inc. v. Visa International Service*

157. *Id.* at 982-83.

158. *Id.* at 983.

159. *Id.* at 984-85.

160. *Id.* at 984 (citing Hard Rock Café Licensing Corp. v. Concession Servs., Inc., 955 F.2d 1143, 1148-49 (7th Cir. 1992)).

161. *Lockheed*, 194 F.3d at 984. The *Lockheed* standard's requirement of "control" has been criticized as an incorrect application of vicarious liability concepts to the realm of contributory liability. *See* Adams, *supra* note 147, at 681-82.

162. *Lockheed*, 194 F.3d at 984-85.

Association.[163] In that case, the plaintiff, the publisher of a subscription website providing photographs of nude models brought claims for contributory trademark infringement against the card associations, Visa and MasterCard, as well as an acquiring bank and payment processor.[164] The plaintiff alleged that after receiving notice of third-party's unauthorized distribution of plaintiff's copyrighted images (which copies also bore the PERFECT 10 trademark), the defendants continued to process payments for those third parties.[165] Applying the test devised in *Lockheed*, the district court dismissed all of the plaintiff's claims under Rule 12(b)(6),[166] and the plaintiff appealed to the Ninth Circuit.

In affirming the district court's dismissal of the plaintiff's claims, the majority agreed that the plaintiff failed to plead sufficient facts to support a contributory infringement claim under the *Lockheed* standard. The widespread use of credit cards for Internet transactions was not lost on the majority, which acknowledged that "credit cards serve as the primary engine of electronic commerce."[167] Nevertheless, the majority did not consider the infringement – unauthorized distribution – to be dependent on the direct infringers' ability to accept credit card payments; that is, the infringing photographs could be distributed whether or not a sale was completed using a credit card, or at all.[168] This led the majority to the critical (and for

163. 494 F.3d 788 (9th Cir. 2007).

164. *Id.* at 793.

165. *Id.*

166. Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 73 U.S.P.Q.2d 1736 (N.D. Cal. 2004).

167. Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 794 (9th Cir. 2007).

168. *Id.* at 807. In reaching its conclusions as to the instrumentality of infringement for purposes of contributory trademark infringement, the majority incorporates (without reference) its rationale "[a]s discussed at length above." *Id.* The most reasonable interpretation is that the majority is referring to prior statements made in the context of contributory copyright infringement, such as "Perfect 10 has not alleged that any infringing material passes over Defendants' payment networks or through their payment processing systems," and "[w]hile Perfect 10 has alleged that Defendants make it easier for websites to profit from this infringing activity, the issue here is reproduction, alteration, display and distribution, *which can occur without payment*." *Id.* at 796 (emphasis added). These statements coincide with the majority's view that the payment network is neither involved in nor

plaintiff, fatal) holding that it was the infringing websites, not the defendants' payment network, or any combination of the two, that was the "instrumentality used to infringe the plaintiff's mark."[169] Having thus defined the instrumentality of infringement, the Court continued to note that the defendant card associations and payment processors were not alleged to have "the power to remove infringing material from these websites or directly stop their distribution over the Internet."[170] While the defendants did have the ability to cease processing payments, which might stop or reduce the infringements (or might not, as the majority stressed throughout its opinion[171]), the defendants did not exercise the "direct control" over the instrumentality, as required by *Lockheed*.[172]

Circuit Judge Alex Kozinski wrote an impassioned dissent in *Perfect 10*, arguing that because "credit cards are directly involved in every infringing transaction," the defendants effectively "control whether such transactions will go forward."[173] Where the majority sought to divorce the "means of payment" from the "mechanics of transferring the material," Kozinski colorfully argued that "[i]n a commercial environment, distribution and payment are . . . like love and marriage-you can't have one without the other."[174] This, Judge Kozinski believed, was control enough for the plaintiff to satisfy the *Lockheed* test and survive a motion to dismiss.[175] (However, Judge Kozinski did note that, given the defendants' differing roles in processing payments, the ultimate question of liability could turn on whether the defendants had direct

essential to the alleged infringements.

169. *Id.* at 807.

170. *Id.*

171. *See, e.g.*, *id.* at 796, 798, 807.

172. *Id.* at 807. Among the criticisms of *Perfect 10* is the majority's failure to distinguish between the card association defendants, the acquiring bank defendant, and processor defendant – all of whose relationships to the direct infringers differ. *See, e.g., id.* at 811 n.2 (noting "simplifying assumptions" used by majority); Kelly K. Yang, *Paying for Infringement: Implicating Credit Card Networks in Secondary Trademark Liability*, 26 BERKELEY TECH. L.J. 687, 706-10 (2011).

173. 494 F.3d at 821 (Kozinski, J., dissenting).

174. *Id.* at 818 (Kozinski, J., dissenting).

175. *Id.* at 822 (Kozinski, J., dissenting).

relationships with the infringing merchants).[176] The Kozinski dissent would be influential the next time contributory infringement claims were levied against payment processors.

b. Gucci v. Frontline Processing Corp.

Where *Perfect 10* marked an outright victory for payment processors, the Southern District of New York's recent decision in *Gucci America, Inc. v. Frontline Processing Corp.*[177] introduces uncertainty. In *Frontline*, luxury goods manufacturer Gucci America, Inc., having first obtained judgment against "Laurette," an internet seller of replica GUCCI products,[178] brought suit against two acquiring banks and/or payment processors,[179] Frontline Processing Corp. and Woodforest National Bank, as well as Durango Merchant Services LLC, an alleged agent aiding the processors in locating merchants.[180]

The three named defendants were alleged to have supplied credit card processing services for Laurette, enabling sales of counterfeit goods through the website TheBagAddiction.com.[181] Durango was found to have "specializ[ed] in services for 'High Risk Merchant Accounts'"[182] such as sellers of replica goods.[183]

176. *Id.* at 811 n.2 (Kozinski, J., dissenting). This observation suggests the possibility of different outcomes between card associations and acquiring banks/payment processors in four-party systems, as well as between card associations in four-party and three-party systems (e.g., Visa and MasterCard).

177. 721 F. Supp. 2d 228 (S.D.N.Y. 2010).

178. *See* Gucci America, Inc. v. Laurette Co., No. 08-cv-5065 (LAK) (S.D.N.Y. Jun. 3, 2008).

179. *See Frontline Processing Corp.*, 721 F. Supp. 2d at 239 n.3 ("Neither party has provided sufficiently clear terminology to describe Woodforest or Frontline. For the purposes of this opinion, terms like 'acquiring bank' and 'credit card processors' are intended to have the same meaning and do not imply anything about their services beyond what is alleged in the complaint.").

180. *Id.* at 238.

181. *Id.* at 239.

182. *Id.* at 238. It is not uncommon for those catering to high-risk merchants to specifically reference "replica products" in their literature. *See, e.g.*, PAINLESS PROCESSING, http://www.painlessprocessing.com/replica-merchant-account.php (last visited Mar. 7, 2012) ("We at Painless Processing specialize in getting our clients approval for high risk merchant accounts

In providing these services to Laurette, Durango allegedly devised a system designed to aid Laurette in avoiding chargebacks, which the court construed as "'affirmative steps taken to foster infringement.'"[184] The court concluded that, as to Durango, Gucci had sufficiently pleaded a claim for relief under the inducement prong of *Inwood*.[185]

The district court, noting that the Second Circuit had not adopted *Lockheed* – or what it deemed the modified part of the *Inwood* test – nevertheless found it a "persuasive synthesis" for adjudging allegations of contributory trademark infringement against service providers such as Frontline and Woodforest.[186] However, the court set forth an arguably relaxed version of the *Lockheed* test, assessing contributory liability by evaluating whether Frontline and Woodforest "knowingly supplied services to websites and had *sufficient* control over infringing activity to merit liability."[187]

Frontline and Woodforest's knowledge of Laurette's infringement was established by their involvement in reviewing Laurette's website and investigating consumer

including replica merchant accounts."); REPLICA MERCHANT ACCOUNTS, MerchantAccount-highrisk.com, http://merchantaccount-highrisk.com/replica-merchant-account.html (last visited Mar. 7, 2012) ("Need a merchant account for a replica merchandise business? Then you need a high risk, replica merchant account . . . .We can enable you to process payments."); *When a Web-Based Business Needs Replica Merchant Account,* GSPAY.COM, http://www.gspay.com/when-a-web-based-business-needs-replica-merchant-account.php (last visited Mar. 7, 2012) ("Online merchant account will give you complete independence. It will help make your web replica business more successful and profitable. . . . Boost the potential of your business with replica merchant account!").

183. 721 F. Supp. 2d at 238.

184. *Id.* at 249.

185. *Id.*

186. *Id.* at 248 (quoting Tiffany (NJ) Inc. v. eBay, Inc., 576 F. Supp. 2d 463, 504 (S.D.N.Y. 2008)); *see also* Tiffany (NJ) Inc. v. eBay, Inc., 600 F.3d 93, 105-06 (2d Cir. 2010) ("We therefore assume without deciding that *Inwood's* test for contributory trademark infringement governs.").

187. 721 F. Supp. 2d at 248 (emphasis added); The court reiterates the standard as requiring sufficient control. *Id*. at 249. The court later states that "[p]laintiff provides sufficient factual allegations to establish a claim that Woodforest and Frontline had *some control* over the directly infringing third-party, but fails to provide enough facts to show control on the part of Durango." *Id.* at 251 (emphasis added).

chargebacks for items purchased from TheBagAddiction.com.[188] As to the control element, the court defined the instrumentality of infringement as "the combination of the website and the credit card network, since both are allegedly necessary elements for the infringing act."[189] The court draws heavily from Judge Kozinski's dissent in *Perfect 10* to establish the interconnectedness of the website and payment network, reasoning that "[i]f, as Gucci alleges, the Laurette website was functionally dependent upon Woodforest and Frontline's credit card processing services to sell counterfeit Gucci products, it would be sufficient to demonstrate the control needed for liability."[190]

Interestingly, the *Frontline* court follows Judge Kozinski's reasoning in holding that distribution and payment are inseparable (like love and marriage), while also accepting, or at least not explicitly rejecting, the *Perfect 10* majority's conclusion that the two may be separable.[191] In so holding, the *Frontline* court distinguishes *Perfect 10*: "the infringing conduct [in *Perfect 10*] was the publication *on the website* of trademarked images of nude models, and the distribution occurred via individuals viewing and taking the image directly from the website."[192] If *Perfect 10* and *Frontline* are to be read as consistent with one another, it would seem that the different outcomes hinge on whether the directly infringing product is non-rivalrous (*Perfect 10*) or rivalrous (*Frontline*).[193] That is, it is conceivable that the *Perfect 10* infringers could continue to distribute free electronic copies of the infringing photos, as doing so would not impair their ability to meet paying customers' demand for electronic copies. In contrast, because the *Frontline* direct infringer, Laurette, dealt in physical goods, it would be far less likely to distribute products without a functional payment network.

188. *Id.* at 249-50.
189. *Id.* at 252.
190. *Id.* at 253.
191. *Id.* at 252.
192. *Id.*
193. Eric Goldman, *Payment Service Providers May Be Liable for Counterfeit Website Sales*--Gucci v. Frontline, ERIC GOLDMAN TECH. & MARKETING L. BLOG (June 29, 2010, 12:19 PM), http://blog.ericgoldman.org/archives/2010/06/payment_service.htm.

Thus, Gucci was able to defeat a motion to dismiss its claims for contributory infringement against Durango (inducement theory) and Frontline and Woodforest (knowing supply of services theory). However, *Frontline* did not result in a finding of contributory liability against any of the defendants, since the parties settled out of court.[194] But in finding that Gucci had stated claims for contributory infringement against the defendant payment processor, acquiring bank, and agent, *Frontline* introduces uncertainty for payment processors as to their legal obligations and potential liabilities. *Frontline* suggests that card networks such as American Express and Discover, which themselves perform the functions performed by acquiring banks in four-party systems may be susceptible to claims for contributory liability for the infringements of their merchants. *Frontline* even leaves open the possibility of liability for card associations such as Visa and MasterCard, despite their lack of direct relationships with infringing merchants.

C. *Credit Card Associations' Cooperation with Brand Owners*

1. Card Associations' Voluntary Anti-Counterfeiting Policies

Card associations have incentives for keeping unsavory or criminal merchants from plying their trade through the associations' payment networks. In some cases, as with internet gambling, the incentive is to avoid indirect liability under the Unlawful Internet Gambling Enforcement Act (UIGEA)[195] by "establish[ing] and implement[ing] written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit" use of the payment networks for internet gambling.[196]

194. Final Order and Judgment on Consent at 1-2, Gucci America, Inc. v. Frontline Processing Corp., 721 F. Supp. 2d 228 (S.D.N.Y. 2010) (No. 09-cv-6925), *available at* http://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2009cv06925/350358/90/0.pdf?ts=1286286153.

195. Unlawful Internet Gambling Enforcement Act of 2006, Pub. L. No. 109-347, 120 Stat. 1884 (codified at 31 U.S.C. §§ 5361 – 5367 (2006)).

196. 12 C.F.R. § 233.5(a) (2009). For a discussion of the UIGEA and the

Even where the law might not impose such a direct duty, Visa and MasterCard – brand owners themselves – have incentives to protect the goodwill embodied by their trademarks. To that end, both card associations impose duties on their acquiring banks to restrict merchant activity. For example, MasterCard prohibits "[i]llegal or [b]rand-damaging transactions," including "[t]he sale or offer of sale of a product or service other than in full compliance with the law."[197] Likewise, Visa's Operating Regulations prohibit use of the Visa network for illegal activities which include, but are not limited to, child pornography, money laundering or financing terrorist activities.[198] Though it presumably falls within each card association's definition of "illegal" transactions,[199] the sale of counterfeit goods is not explicitly mentioned in either card association's rules.

Despite the absence of an explicit prohibition on merchants' trafficking in counterfeit goods, both Visa and MasterCard have policies in place that allow brand owners to notify the card associations of websites that accept, or purport to accept, their payment cards to purchase counterfeit goods. So, rather than sue, brand owners can seek Visa and MasterCard's assistance in cutting off payment processing services to websites selling counterfeit goods by submitting reports of intellectual property infringement. For reports submitted to Visa and MasterCard, brand owners must provide a description of the alleged violation, provide their contact information (and that of their agent, if applicable), identify the

system adopted by card networks to identify and block internet gambling transactions, see Mark MacCarthy, *What Payment Intermediaries Are Doing About Online Liability and Why It Matters*, 25 BERKELEY TECH. L.J. 1037, 1062-66 (2010).

197. MASTERCARD WORLDWIDE, MASTERCARD RULES § 5.11.7 (Feb. 24, 2012), *available at* http://www.mastercard.com/us/merchant/pdf/BM-Entire_Manual_public.pdf.

198. VISA, VISA INTERNAL OPERATING REGULATIONS 786 (Apr. 15, 2012), *available at* http://usa.visa.com/download/merchants/visa-international-operating-regulations-main.pdf [hereinafter VISA OPERATING].

199. Sales of counterfeit goods have been identified as a source of income for terrorist organizations. *Counterfeit Goods are Linked to Terror Groups - Business - International Herald Tribune*, N.Y. TIMES (Feb. 12, 2007), http://www.nytimes.com/2007/02/12/business/worldbusiness/12iht-fake.4569452.html.

intellectual property that is allegedly infringed, and provide the allegedly infringing merchant's name, website, and country, if available.[200] On this last point – identifying the merchant – it is sufficient to provide Visa and MasterCard with the domain name of the infringing site, and the registrant's contact information contained in the Whois record for that domain name. Of course, there must also be a basis for believing that a reported website accepts the relevant type of credit card, which can be satisfied by a screenshot or a representation that the website claims to accept VISA or MASTERCARD credit cards.

Upon receipt of a report of intellectual property infringement, the card association will conduct a test transaction for each identified website. This allows the card association to verify that the website does in fact transact business over its payment network, and to identify the acquiring bank handling the merchant account. The card association will then instruct the acquiring bank to investigate the activities of the merchant associated with the website.[201] In the Visa and MasterCard networks, presuming the acquiring bank determines that a violation has occurred and absent "compelling" evidence to the contrary, the bank is expected to terminate the merchant account,[202] and enter the merchant's information into the MATCH system so that other acquiring banks may be notified of the merchant's past transgressions.[203]

200. *Intellectual Property Rights*, VISA INC., http://corporate.visa.com/about-visa/security-and-trust/intellectual-property-rights.shtml (last visited Mar. 13, 2012) [hereinafter VISA IP].

201. *See, e.g.*, *id.*; *MasterCard Anti-Piracy Policy*, MASTERCARD WORLDWIDE, http://www.mastercard.com/us/wce/PDF/MasterCard_Anti-Piracy_Policy.pdf [hereinafter *MasterCard Anti-Piracy*).

202. *MasterCard Anti-Piracy*, *supra* note 201.

203. MATCH stands for "Member Alert to Control High-Risk (Merchants)." MASTERCARD WORLDWIDE, SECURITY RULES AND PROCEDURES: MERCHANT EDITION 11-i (Feb. 24, 2012), *available at* http://www.mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdfhttp://www.mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdf. MATCH is a database containing information about terminated merchants, including name, address and other identifiable information. Under both the Visa and MasterCard systems, acquiring banks are required to consult MATCH as part of their investigation into potential merchants. *Id.* at 11-5http://www.mastercard.com/us/merchant/pdf/SPME-

The results of the investigation (e.g., claiming that a merchant account has been terminated) are then reported to the brand owner who submitted the complaint.

In the absence of any legislation or case law that unequivocally imposes on the card associations a duty to monitor their payment networks to prevent counterfeit transactions, the above-described policies may be considered "voluntary." However, one can reasonably presume that these voluntary anti-counterfeiting policies are in part defensive, aimed at staving off lawsuits and potential adverse judicial decisions imposing secondary liability, and providing a basis for card associations to argue to legislators that legislation (such as that discussed in Part IV) is unnecessary.[204] But whatever the reason, or the degree of volition, card associations presently appear willing to assist brand owners in combating online infringement.

The recent evolution of the card associations' policies seems to support the view that they are a reaction to pending legislation and/or the *Frontline* decision. In September 2009, the International Trademark Association (INTA) released "Addressing the Sale of Counterfeits on the Internet," a document setting forth voluntary best practices for brand owners and "Payment Service Providers" (PSPs) in jointly combating online counterfeit sales.[205] In addition to providing the PSP with information such as the infringing URL, and proof of the brand owner's intellectual property rights, these best practices contemplated imposing on brand owners the duty to complete a purchase from the alleged counterfeiter, and

Entire_Manual_public.pdfhttp://usa.visa.com/download/merchants/visa-international-operating-regulations-main.pdf, VISA OPERATING, *supra* note 198, at 852-54. Acquiring banks are required to input into MATCH information regarding merchants who are terminated as a result of brand owners' intellectual property reports. *See, e.g.*, *MasterCard Anti-Piracy Policy*, *supra* note 201.

204. Yang, *supra* note 172, at 719.

205. INTERNATIONAL TRADEMARK ASSOCIATION, ADDRESSING THE SALE OF COUNTERFEITS ON THE INTERNET (Sept. 2009), *available at* http://www.inta.org/Advocacy/Documents/INTA%20Best%20Practices%20for%20Addressing%20the%20Sale%20of%20Counterfeits%20on%20the%20Internet.pdf.

to agree to indemnify[206] the PSP for any liabilities incurred from terminating services to a merchant based on the brand owner's complaint.[207] Until recently, Visa required the brand owner to make a purchase from the alleged infringer in order to identify the acquiring bank. For its part, MasterCard required the brand owner's agreement to indemnify MasterCard, plus to pay a per-URL fee. None of these requirements exist under MasterCard or Visa's current policies.[208] To the extent that the cost of conducting purchases, or reservations about providing indemnity, dissuaded brand owners from working with the card associations' voluntary policies, these requirements are no longer obstacles.

Card associations and payment processors have also evinced a willingness to assist brand owners in other ways. For example, Visa International, Visa Europe, MasterCard, PayPal, and American Express have all signed on to participate in the International Anticounterfeiting Coalition's (IACC) "payment processor portal."[209] The IACC "portal," which

206. Among other things, the call for indemnification arises out of Visa's experience with the Russian website AllofMP3.com. Acting upon a complaint that AllofMP3.com provided unauthorized downloads of copyrighted music to consumers in whose jurisdictions such downloads were infringing, Visa advised the Russian acquiring bank to terminate the Visa merchant account. The merchant then sued the acquirer for breach of the merchant agreement, Visa intervened in the suit on behalf of the acquirer, and a Russian court decided in favor of the merchant, ordering that the bank and network continue processing payments. This example of the application of sometimes incongruous national laws to global transactions is one way that card associations are exposed to potential liability in acting upon brand and content owner's infringement complaints. *See Targeting Websites Dedicated To Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 7-9 (2011) (statement of Denise Yee, Visa Inc.); MacCarthy, *supra* note 196, at 1093-95.

207. *Targeting Websites Dedicated To Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 6 (2011) (statement of Denise Yee, Visa Inc.).

208. *MasterCard Anti-Piracy Policy*, *supra* note 201; VISA IP, *supra* note 200. However, indemnity has not been totally abandoned, and may still be required where, in investigating complaints of infringement, "undue risk will be shifted to Visa were [Visa] to decide in favor of the intellectual property owner." *Targeting Websites Dedicated To Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 14 (2011) (statement of Denise Yee, Visa Inc.).

209. Int'l Anticounterfeiting Coal., Address at LVMH Tower Regarding IACC Payment Processor Portal (Oct. 12, 2011).

launched in early January 2012, is a web-based tool which allows participating brand owners to submit a single report of infringement to all participating payment processors.[210] In theory, the IACC portal should increase efficiency by obviating the need for brand owners to submit a separate complaint to each payment processor, and by reducing redundancies, such as where a processor must act on multiple complaints from different brand owners concerning the same URL.[211] However, unlike the card associations' individual policies, use of the IACC portal is not open to the public.[212] The IACC assesses an annual fee for access to the portal[213] which, of course, must be factored into brand owners' cost-benefit analysis. Finally, the third party retained to administer the IACC portal boasts numerous financial institutions among its existing clients, and brand owners contemplating using the IACC portal should keep in mind this shared loyalty.[214]

2. Working with the Card Associations

On behalf of several brand owners, the authors of this article have used the infringement reporting policies implemented by Visa and MasterCard. This process has produced mixed results. Visa and MasterCard have provided timely responses to the reports, typically within two weeks (though this timeframe may vary depending on the number of websites identified in a report), resulting in the termination of dozens of merchant accounts associated with counterfeiting websites. And in no case has the associated acquiring bank refused to terminate an identified merchant.

While the card association policies do result in the termination of counterfeiters' merchant accounts, these represent a fairly small percentage of the overall number of websites reported. This is because the majority of websites reported do not actually process payments through the credit card networks advertised on their sites, and are in that respect

210. *Id.*
211. *Id.*
212. *Id.*
213. *Id.*
214. *Id.*

"inactive."[215] That is, although the reported URLs resolve to a functional website, complete with product listings, shopping carts, and, of course, the card associations' logos, it is often impossible to complete a credit card transaction. This inactivity takes two forms: (1) the *website* is inactive, in that a purchase cannot be completed because the website is not working properly, despite all appearances; or (2) the *merchant* is inactive, such that, although a transaction may be authorized, the transaction is not submitted by the merchant into the payment system for clearing and settlement.[216] Surprisingly, an overwhelming majority of sites most highly ranked (i.e., on the first few pages) in search engines' organic results over a period of 1-2 months have proven "inactive" upon investigation. Though the high incidence of inactive websites was unexpected, it was encouraging to learn that while such web sites may attract consumers, these attractions cannot end in completed sales of counterfeit product.

Of course, a finding of inactivity does not guarantee that a website cannot resume actively accepting credit card payments by obtaining a new account with a different acquiring bank. And because there is no visible indication that activity has resumed – the merchant does not flip on a neon sign to signal that it is now "ACTIVE" – constant monitoring of the site is required. Card associations have thus far been amenable to re-testing sites previously deemed inactive, and our results seem to show that, in most cases, sites deemed inactive have remained inactive. Nevertheless, the constant vigilance required to routinely monitor inactive sites and take action against newly registered or discovered websites will lead to ever-increasing watch lists for brand owners. To help alleviate this burden, enforcement through card associations' voluntary policies should be coupled with enforcement efforts that result in the websites being seized or otherwise made inaccessible to

215. As used throughout this section, the terms "active" and "inactive" will refer to the ability and inability, respectively, to accept a credit card for purchases.

216. In some instances, these sites may be phishing sites, designed solely to misappropriate a consumer's personal and credit card information. A consumer may believe he is inputting his credit card information to make a purchase, but instead has transmitted personal and financial information to a criminal.

consumers. The mass domain lawsuits discussed in Part II provide a viable option for taking down counterfeiting sites on a large scale, provided the joinder and jurisdictional questions they raise can withstand the scrutiny of the courts, and potential challenges by defendants. And to the extent that they would allow brand owners to affect not only counterfeiters' ability to process payments, but also the accessibility of counterfeiters' sites, legislation of the type described in Part IV (putting aside the constitutional and other concerns raised by opponents) might serve as an effective supplement to, or replacement for, the card associations' voluntary policies.

IV. Legislation Directed Towards Online Piracy and Counterfeits

As brand owners attempt to deal with the problem of online counterfeiting through the courts and through cooperative efforts with credit card associations, lawmakers have been crafting their own solution. Three recent bills in the Senate and House of Representatives have attempted to address online counterfeiting and piracy. The first, the Combating Online Infringement and Counterfeits Act (COICA),[217] was introduced on September 20, 2010 by Senator Patrick Leahy of Vermont, but was quickly stalled in the Senate and expired at the close of the then-current Congressional session. But Senator Leahy was not to be deterred. The following session, Senator Leahy introduced the successor to COICA, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, also known as the PROTECT IP Act, or PIPA.[218] Meanwhile, Representative Lamar Smith of Texas introduced a

217. Combating Online Infringement and Counterfeits Act (COICA), S. 3804, 111th Cong. (2010) [hereinafter COICA I]. Roughly two months later, Senator Leahy introduced an amended version of COICA. Combating Online Infringement and Counterfeits Act, S. 3804, 111th Cong. (as amended by Senate, Nov. 18, 2010) [hereinafter COICA II].

218. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Cong. (2011) [hereinafter PIPA]. An amended version was reported 2 weeks later. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Cong. (as amended by Senate, May 26, 2011).

bill of his own – the Stop Online Piracy Act (SOPA)[219] – in the House of Representatives.

Though by no means identical, COICA, PIPA and SOPA can be considered variations on a common theme, each at its core proposing a framework allowing the Attorney General, and, in the case of PIPA and SOPA, brand and copyright owners, to combat online counterfeiting and piracy through intermediaries whose services enable infringing websites to ply their trade. Notwithstanding their differing terminologies, each proposed to reach four key categories of intermediaries: (1) search engines (e.g., Google and Yahoo!); (2) internet advertising services (e.g., Google Adwords); (3) payment processors (e.g., Visa and MasterCard); and (4) and internet service providers (e.g., Verizon, Comcast). By exploiting counterfeiters' dependence on these intermediaries for survival, the bills' sponsors and supporters hoped to provide brand owners with new, effective tools for combating online counterfeiting.

A. *Summary of the Bills*

COICA, PIPA, and SOPA share a similar basic framework for combating online infringement. Under each bill, counterfeiting websites could be attacked through intermediaries – namely, third parties who provide various services that enable infringing websites to thrive, and on a more basic level, exist. This section will compare the three bills topically, covering the domain names and websites potentially affected; the bills' varying definitions of "infringement"; the third parties through whom plaintiffs would attack infringing sites; the procedures to be employed; and the miscellaneous provisions tacked onto each bill.

219. Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011) [hereinafter SOPA I]. An amended version was introduced two months later. Amendment in the Nature of a Substitute to H.R. 3261, H.R. 3261, 112th Cong. (as amended by House, Dec. 12, 2011) [hereinafter SOPA II].

1. Defining "Infringement"

Both COICA and PIPA were directed at sites "dedicated to infringing activities."[220] COICA defined "dedicated to infringing activities" in several ways. First, the term included sites subject to civil forfeiture under 18 U.S.C. § 2323.[221] Second, the term included sites that were "primarily designed," marketed, or had no "demonstrable, commercially significant" purpose or use other than to infringe copyrights, circumvent protection mechanisms, or sell or distribute counterfeit goods.[222]

PIPA's definition of "dedicated to infringing activities" did not use civil forfeiture as a measuring stick,[223] but is otherwise substantially similar to the "primarily designed" prong of COICA.[224] However, the definition also included websites which *enable* and *facilitate* such infringement,[225] and, in this respect, was likely adopted in lieu of a direct reference to the civil forfeiture statute, which itself covers property used to facilitate the commission of certain intellectual property crimes.[226]

SOPA did not adopt the terminology used by COICA and PIPA, instead setting its sights on two targets: "foreign

220. COICA I, *supra* note 217, § 2(a); PIPA, *supra* note 218, § 2(7); COICA II, *supra* note 217, § 2(a)(1).

221. (a) Civil forfeiture.

> (1) Property subject to forfeiture. The following property is subject to forfeiture to the United States Government:
> (A) Any article, the making or trafficking of which is, prohibited under section 506 of title 17, or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title.
> (B) Any property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense referred to in subparagraph (A).
> (C) Any property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of an offense referred to in subparagraph (A).

18 U.S.C. § 2323(a) (West 2011).

222. COICA I, *supra* note 217, § 2(a).

223. PIPA, *supra* note 218, § 2(7).

224. *Compare* PIPA, *supra* note 218, § 2(7), *with* COICA I, *supra* note 217, § 2(A)(2)(a).

225. PIPA, *supra* note 218, § 2(7).

226. *Id.*

infringing sites" (for purposes of the Attorney General) and "sites dedicated to theft of U.S. property" (for purposes of private plaintiffs). However, SOPA's chosen terms had a similar spirit and scope. "Foreign infringing sites" were defined as those foreign sites directed to the United States, and which would be subject to civil forfeiture if they were domestic sites.[227] SOPA's definition of "sites dedicated to theft of U.S. property" essentially mirrors that of PIPA, including the engage/enable/facilitate triad.[228] Thus, the three bills take slightly different routes to reach the same destination, targeting sites that committed infringements themselves, as well as those that aided others commit infringements, whether they did so with or without actual knowledge of the infringement.

2. Actions Authorized and Domain Names Potentially Affected

All three bills authorize the Attorney General to bring *in rem* actions against domain names associated with infringing websites.[229] PIPA and SOPA also authorize the Attorney General to bring *in personam* actions against the registrants or operators of infringing sites.[230] However, *in personam* actions would likely be rare, given online counterfeiters' proven track record of concealing their true identities and locations, and the strong likelihood that, in any event, they are located outside the United States. Additionally, and in a much more significant way, PIPA and SOPA expanded on COICA by creating a private right of action allowing brand owners and content owners to proceed *in rem* against certain domain names associated with infringing websites.

COICA would have permitted the Attorney General to commence an action against any domain name used in connection with a "site dedicated to infringing activities."[231] In

227. SOPA I, *supra* note 219, §102(a).

228. *Id.* § 103(a)(1).

229. *See* COICA I, *supra* note 217, § 2(c)(1); PIPA, *supra* note 218, § 3(a)(2); SOPA I, *supra* note 219, § 102(b)(2).

230. PIPA, *supra* note 218, § 3(a)(1); SOPA I, *supra* note 219, § 102(b)(1).

231. COICA I, *supra* note 217, § 2(a)(1).

its original and amended forms, COICA places no geographical restrictions on the domain names subject to action.[232] Thus, COICA's reach extended to domains administered and issued by foreign domain name registries and registrars, as well their counterparts residing in the United States.

PIPA circumscribed the Attorney General's powers, limiting actions to those against "nondomestic domain names"[233] – that is, domain names issued and operated by registrars and registries outside the United States.[234] However, PIPA afforded brand owners the same reach that COICA afforded the Attorney General: brand owners were authorized to bring actions against all domain names, regardless of their situs.[235]

SOPA took a similar bifurcated approach. The Attorney General was authorized to act against "foreign infringing sites,"[236] which (in addition to being deemed infringing) had a registrar, registry and IP address located outside the United States.[237] But, like PIPA, SOPA authorized brand owners to act against a broader range of domain names (those associated with sites "dedicated to theft of U.S. property") regardless of their situs.[238] Though SOPA was amended to essentially limit

232. *See* COICA I, *supra* note 217, § 2(a) (where "domain name" is not a defined term), *and* COICA II, *supra* note 217, § 2(a)(2) (adopting definition of "domain name" from 15 U.S.C. § 1127). The Lanham Act defines a domain name as "any alphanumeric designation which is *registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority* as part of an electronic address on the Internet." (emphasis added). Lanham Act, § 45, 15 U.S.C. § 1127 (2006).

233. PIPA, *supra* note 218, § 3(a).

234. PIPA, *supra* note 218, § 2(9). Of course the Attorney General would still be able to act against domestic domain names under the civil forfeiture statute, 18 U.S.C. § 2323, which served as the basis for the Department of Homeland Security Immigration and Customs Enforcement's (ICE) wave of domain seizures beginning in June 2010.

235. PIPA, *supra* note 218, § 4(a); *see also id.* § 2(1) (incorporating definition of "domain name" from 15 U.S.C. § 1127).

236. SOPA I, *supra* note 219, § 102(a).

237. *See generally* SOPA I, *supra* note 219; *see also* definitions of "foreign infringing sites," *id.* § 102(a), "foreign Internet site," *id.* § 101(8), "domestic Internet site," *id.* § 101(5), "domestic domain name," *id.* § 101(3) and "domestic internet protocol address," *id.* § 101(4). But again, the Attorney General's recourse to civil forfeiture proceedings against domestic domain names was unaffected.

238. SOPA I, *supra* note 219, § 103(a).

its reach to foreign sites, brand owners could still use SOPA to reach domains associated with domestic registries and/or registrars, as long as the owner of the site was located outside the United States.[239]

3. Procedures

Upon commencing an action under COICA, the Attorney General could seek relief authorized under Rule 65 of the Federal Rules of Procedure, including a temporary restraining order or preliminary injunction ordering the target to cease its infringing activities.[240] And upon receipt of an order, the Attorney General could serve a copy on certain intermediaries to compel them to take actions to restrict the website's functionality and accessibility. For example, in the case of domestic domains, COICA provided that "[u]pon receipt of such order, the domain registrar or domain name registry shall suspend operation of, and may lock, the domain name."[241] Thus, service of a court order upon the relevant U.S. registrar/registry could disable access to an entire website via the targeted domain name.[242]

For "nondomestic" domain names, the Attorney General's options were different. COICA identified three types of intermediaries that the Attorney General could serve with a court order: (1) "service providers"; (2) "financial transaction providers" ("FTPs"); and (3) "services that provide advertisements to Internet sites" ("Ad Services").[243] Each group was charged with a different set of duties to be performed upon receipt of an order.

239. SOPA II, *supra* note 219, § 103(a)(1). For a definition of a "U.S-directed site", see *id.* § 101(23).

240. COIA II, *supra* note 217, § 2(b).

241. COICA II, *supra* note 217, § 2(e)(1).

242. STEVE CROCKER, ET AL., SECURITY AND OTHER TECHNICAL CONCERNS RAISED BY THE DNS FILTERING REQUIREMENTS IN THE PROTECT IP BILL (2011), *available at* http://www.immagic.com/eLibrary/ARCHIVES/GENERAL/SHNKROUS/S110525C.pdf.

243. COICA II, *supra* note 217, § 2(e)(2).

COICA defined "service providers" broadly, incorporating the meaning ascribed to that term in 17 U.S.C. § 512(k)(1),[244] as well as encompassing "any other operator of a nonauthoritative domain name system."[245] Upon receipt of an order, a service provider (such as Comcast, Verizon, and other ISPs) would be required to take "technically feasible and reasonable steps designed to prevent a domain name from resolving to that domain name's Internet protocol address."[246] FTPs (such as Visa and MasterCard), defined with reference to 31 U.S.C. § 5362(4),[247] would be required to take "reasonable measures . . . designed to prevent or prohibit [their] services from completing payment transactions" between the site and U.S. customers.[248] Finally, Ad Services that supplied advertisements to the website were to cease doing so upon receipt of the court order.[249]

244. (k) Definitions.

(1) Service provider.

(A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

(B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

17 U.S.C. § 512(k)(1) (2010).

245. COICA I, *supra* note 217, § 2(e)(2). "Nonauthoritative domain name system server" is not defined in the original or amended versions of COICA. It is, however, defined in the Stop Online Piracy Act as "a server that does not contain complete copies of domains but uses a cache file that is comprised of previous domain name server lookups, for which the server has received an authoritative response in the past." SOPA I, *supra* note 219, § 101(19).

246. COICA II, *supra* note 217, § 2(e)(2)(B)(i).

247. 31 U.S.C. § 5362(4) (2006). ("(4) Financial transaction provider. The term 'financial transaction provider' means a creditor, credit card issuer, financial institution, operator of a terminal at which an electronic fund transfer may be initiated, money transmitting business, or international, national, regional, or local payment network utilized to effect a credit transaction, electronic fund transfer, stored value product transaction, or money transmitting service, or a participant in such network, or other participant in a designated payment system.").

248. COICA II, *supra* note 217, § 2(e)(2)(B)(ii).

249. COICA I, *supra* note 217, § 2(e)(2)(B)(iii).

PIPA and SOPA operated in much the same way, but with slight variations. For example, PIPA did away with COICA's expansive definition of "service provider." In its place, PIPA referred simply to "operators of a nonauthoritative domain name system server" ("DNS Operators").[250] And in addition to DNS Operators, FTPs, and Ad Services, all of which had analogues under COICA, PIPA identified a fourth discrete category of intermediaries on whom the Attorney General might serve an order: "information location tools,"[251] i.e., search engines. Upon receipt of an order, information location tools would be required to take reasonable measures to "(i) remove or disable access to the Internet site associated with the

250. PIPA, *supra* note 218, § 3(d)(2)(A)(i).

251. PIPA, *supra* note 218, § 3(d)(2)(A). (the term "information location tool" is a defined term); *see also* PIPA, *supra* note 218, § 2(4). PIPA draws upon 17 U.S.C. § 512(d):

> (d) Information location tools. A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider—
> (1) (A) does not have actual knowledge that the material or activity is infringing;
> (B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
> (C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
> (2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
> (3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.

17 U.S.C. § 512(d) (2010).

domain name . . . or (ii) not serve a hypertext link to such Internet site."[252] Thus, in addition to terminating a website's ability to process payments, depriving it of its advertisements and associated revenue, and blocking DNS translation of the associated domain name, the Attorney General could also demand that a nondomestic domain be de-indexed from search engine results. Private actors were limited to compelling action by only FTPs and Ad Services.[253]

SOPA provided slightly different terminology and definitions, but essentially affected the same types of intermediaries.[254] Far more notable was the "Market-Based System to Protect U.S. Customers and Prevent U.S. Funding of Sites Dedicated to Theft of U.S. Property" that appeared in the original version of SOPA.[255] This so-called market-based system called for the creation of a DMCA-like notice/counter notice framework to be used by brand owners prior to, and as a prerequisite for, seeking a court order to compel action by FTPs and Ad Services.[256] A plaintiff would serve a "notification regarding internet sites dedicated to theft of U.S. property" upon the agent designated by the intermediary. The recipient intermediary was required to notify the alleged infringer and take "technically feasible and reasonable measures" within no more than five days to suspend their services.[257] FTPs were tasked with preventing the infringing site from completing payment transactions with consumers in the United States.[258] Ad Services were to cease providing advertisements to or for the infringing site, and cease providing or receiving ad revenue

252. PIPA, *supra* note 218, § 3 (d)(2)(D).

253. PIPA, *supra* note 218, § 4(d)(2).

254. For example, PIPA defined FTPs with reference to 31 U.S.C. § 5362(4). SOPA speaks of "payment network providers," meaning those who "directly or indirectly provide[] the proprietary services, infrastructure, and software to effect or facilitate a debit, credit, or other payment transaction." SOPA II, *supra* note 219, § 101(20)(a). In addition, SOPA uses the term "internet search engine" in place of PIPA's "information location tool," and defines it differently. *Compare* SOPA II, *supra* note 219, § 101(15), *with* PIPA, *supra* note 218, § 2(4), *and* 17 U.S.C. § 512(d) (2010).

255. SOPA I, *supra* note 219, § 103.

256. *Id.* § 103(b).

257. *Id.* § 103(b)(1)-(3).

258. *Id.* § 103(b)(1).

derived from the infringing site.[259] If the recipient intermediary did not take appropriate action in response to the notice, or resumed supplying services upon receipt of a counter-notice from the alleged infringer, *then* the brand owner could commence an action and obtain an order compelling the third party to take action under the same framework set out in COICA and PIPA.[260]

4. Safe Harbors

Each bill afforded immunities to the third-party services providers compelled to take action against infringing sites. COICA provided immunity to these various third-party service providers for taking actions "reasonably designed to comply" with an order.[261] COICA also provided immunity in instances where a third-party service provider voluntarily ceased providing its services to a website it "reasonably believe[d]" was dedicated to infringing activities.[262] However, in the event that a third-party service provider "knowingly and willfully" failed to take appropriate action in response to an order, the Attorney General was entitled to seek injunctive relief to compel compliance.[263] Likewise, Section 5 of PIPA provided immunity to third-party service providers for voluntary actions taken "in good faith and based on credible evidence" against sites reasonably believed to be dedicated to infringing activities.[264] PIPA also extended that immunity to actions taken against sites "engaged in infringing activities that endanger the public health."[265] Similar safe harbors were provided under SOPA.

259. *Id.* § 103(b)(2).
260. *Id.* § 103(c).
261. COICA II, *supra* note 217, § 2(e)(5)(A).
262. *Id.* § 2(e)(5)(B) (this subsection did not appear in the original bill, COICA I).
263. *Id.* § 2(g)(1).
264. PIPA, *supra* note 218, § 5(a).
265. *Id.* § 5(b).

5. Miscellaneous Provisions

In its original form, COICA contained a subsection (j) which provided that the Attorney General would "maintain a public listing of domains that, upon information and reasonable belief, the Department of Justice determines are dedicated to infringing activities but for which the Attorney General has not filed an action under this section."[266] Service providers, FTPs, and Ad Services were encouraged to voluntarily deny their services to sites identified on the Attorney General's list, and offered similar safe harbors as applied to actions compelled by order.[267] Subsection (j) also set out procedures for website owners/operators to petition the Attorney General to have their sites removed from the list, and for judicial oversight of the Attorney General's decisions on such petitions.[268] Not surprisingly, Subsection (j) led opponents to dub COICA as an "internet blacklist" bill.[269] This provision did not appear in the amended version of COICA.

For its part, SOPA also proposed a number of amendments to Titles 17 and 18, as well as provisions for dealing with "notorious foreign infringers," and defending IP rights abroad.[270] Among the more controversial (and unrelated to counterfeiting) was a provision tightening restrictions on online streaming of copyrighted content.[271] Opponents dubbed this the "Free Bieber" provision, alluding to pop star Justin Bieber's rise to fame, which had its roots in his unauthorized YouTube video performances of copyrighted musical compositions.[272]

266. COICA I, *supra* note 217, § 2(j).

267. COICA I, *supra* note 217, § 2(j)(2).

268. *Id.* § 2(j)(3)-(4).

269. David Segal & Aaron Swartz, *Stop the Internet Blacklist*, HUFFINGTON POST (Sept. 27, 2010, 9:40 AM), http://www.huffingtonpost.com/david-segal/stop-the-internet-blackli_b_739836.html.

270. SOPA II, *supra* note 219, §§ 201-205.

271. *Id.* § 201.

272. Amy Schatz, *What Is SOPA Anyway? A Guide to Understanding the Online Piracy Bill*, WALL ST. J. (Jan. 18, 2012), http://online.wsj.com/article/SB10001424052970203735304577167261853938938.html.

B. *Objections to the Proposed Legislation*

The Senate Judiciary Committee unanimously approved COICA on November 18, 2010.[273] Eleven days later, Senator Ron Wyden (D-OR) placed a hold on the legislation, writing that COICA "attempts to protect intellectual property in the digital arena in a way that could trample free speech and stifle competition and important new innovations in the digital economy."[274] With the Wyden hold in place, COICA died at the close of the Congressional session. Senator Wyden similarly placed a hold on PIPA in the Senate,[275] and vowed to filibuster PIPA if the hold were lifted.[276] Senator Wyden wrote of PIPA,

> I understand and agree with the goal of the legislation, to protect intellectual property and combat commerce in counterfeit goods, but I am not willing to muzzle speech and stifle innovation and economic growth to achieve this objective. At the expense of legitimate commerce, PIPA's prescription takes an overreaching approach to policing the Internet when a more balanced and targeted approach would be more effective. The collateral damage of this approach is speech, innovation and the very integrity of the Internet.[277]

Technology companies such as Google and Facebook, who likely would be directly affected by passage of the bills, shared

273. Sam Gustin, *Web Censorship Bill Sails Through Senate Committee*, WIRED.COM (Nov. 18, 2010, 2:50 PM), http://www.wired.com/epicenter/2010/11/coica-web-censorship-bill/all/1.

274. Ron Wyden, U.S. Senator from Oregon, Statement by Senator Ron Wyden Objecting to Unanimous Consent to Proceed to the Combating Online Infringement and Counterfeits Act (Nov. 29, 2010), *available at* http://wyden.senate.gov/imo/media/doc/Statement%20on%20COICA%20hold.pdf.

275. Press Release, U.S. Senator Ron Wyden, Wyden Places Hold on Protect IP Act (May 26, 2011), *available at* http://wyden.senate.gov/newsroom/press/release/?id=33a39533-1b25-437b-ad1d-9039b44cde92.

276. David Kravets, *Senator Threatens to Filibuster Internet Blacklisting Bill*, WIRED.COM (Nov. 21, 2011, 4:56 PM), http://www.wired.com/threatlevel/2011/11/wyden-pipa-filibuster/.

277. Wyden Places Hold on Protect IP Act, *supra* note 275.

Wyden's opposition. In a letter to members of Congress published in the *New York Times* in November 2011, Silicon Valley rivals joined forces to voice concerns that PIPA and SOPA created "uncertain liabilities," required "monitoring of websites," threatened cybersecurity, and undermined the Digital Millennium Copyright Act (DMCA).[278]

On January 14, 2012, the Obama Administration announced its opposition to PIPA and SOPA: "[W]e will not support legislation that reduces freedom of expression, increases cybersecurity risk, or undermines the dynamic innovative global internet."[279] The Obama administration advocated for more narrowly tailored legislation, and encouraged brand and content owners and service providers to work cooperatively.[280] Days later, on January 18, 2012, thousands of websites, including Wikipedia and Mozilla, went "dark" in a massive coordinated protest of PIPA and SOPA.[281] The blackout of these websites was intended to provide internet users with a "visceral example" of what website operators feared might result (i.e., the forced shut down of their website) should either bill be passed.[282] The online protests were accompanied by physical demonstrations in cities such as New York, where protestors assembled outside of Congressional offices.[283]

278. *We Stand Together to Protect Innovation*, N.Y. TIMES, Nov. 16, 2011, at A11.

279. Victoria Espinel, Aneesh Chopra & Howard Schmidt, *Official White House Response to Stop the E-PARASITE Act and 1 other petition: Combating Online Piracy while Protecting an Open and Innovative Internet*, WE THE PEOPLE, https://wwws.whitehouse.gov/petition-tool/response/combating-online-piracy-while-protecting-open-and-innovative-internet.

280. *Id.*

281. Zach Carter & Ryan Grim, *SOPA Blackout Aims to Block Internet Censorship Bill*, HUFFINGTON POST (Jan. 18, 2012, 12:01 AM), http://www.huffingtonpost.com/2012/01/18/sopa-blackout-internet-censorship_n_1211905.html.

282. Jon Swartz & Scott Martin, *Proposals Spur Website Protests*, USA TODAY, Jan. 18, 2012, at B1, *available at* http://www.usatoday.com/MONEY/usaedition/2012-01-18-SOPA-Protest_ST_U.htm (quoting Rob Berschizze, Managing Editor, *Boing Boing*).

283. Carter & Grim, *supra* note 281.

Following the outpouring of opposition, both houses of Congress delayed further action on the bills indefinitely.[284] The following sections will highlight some of the more prominent objections underlying the protests, which remain relevant even as the bills' support in Congress waned, then vanished.

1. Creation of a Duty to Monitor

On any given day, sites such as YouTube provides access to numerous videos that incorporate copyrighted materials without authorization. While many are clearly fair uses, many are clearly infringements. Likewise, a large number of items sold or offered for sale on auction sites like eBay are counterfeit. To date, YouTube, eBay, and many others have avoided liability in the United States for their roles in providing access to infringing content and counterfeit products, because they contend that until notified of a specific instance of infringement, they do not truly know whether a particular item is infringing. The Court of Appeals for the Second Circuit and District Court for the Southern District of New York (among others) have endorsed this theory, holding that "generalized knowledge" that infringements may be occurring on an online platform does not subject the operator to contributory liability for trademark or copyright infringement.[285] Opponents of PIPA and SOPA argue that the proposed legislation would impose on eBay and YouTube (and like platforms) a duty to monitor their systems for infringing content and counterfeit products, or else face termination of services and shuttering of their sites.[286] Imposing such a duty runs counter to current contributory liability case law, and, some argue, serves as an end-around to the DMCA's safe harbor provision.

284. Michael Macleod-Ball, *SOPA and PIPA Votes Delayed Indefinitely*, ACLU (Jan. 20, 2012, 11:52 AM), http://www.aclu.org/blog/free-speech-technology-and-liberty/sopa-and-pipa-votes-delayed-indefinitely.

285. Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93, 109 (2d Cir. 2010) (stating that allegations failed to provide sufficient knowledge under *Inwood*); Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 525 (S.D.N.Y. 2010).

286. *We Stand Together to Protect Innovation*, N.Y. TIMES, Nov. 16, 2011, at A11.

Under current law, when notified of specific instances of infringement, eBay and YouTube take action to remove infringing items to escape liability. YouTube, because it deals in copyrighted content, relies on the provisions of the Digital Millennium Copyright Act.[287] The DMCA provides a safe harbor for hosts of websites that publish materials that infringe a party's copyright, provided that, upon notice from the copyright owner, the content host promptly disables access to the infringing materials.[288] The DMCA has been interpreted to mean that a host cannot be liable for its failure to act upon *general* knowledge that its site *may* be offering infringing material, so long as it doesn't take an active role in the infringing activity, and upon notice of actual infringing material residing on its website, promptly disables the infringing content.[289] For this reason, despite the fact that it knows its site is used by many to post infringing videos, a site like YouTube cannot be held liable because upon notice of any specific infringing video, it takes prompt measures to remove the video.[290]

Although trademark law does not have an analogous statutory safe harbor, similar common law principles apply. Currently, contributory trademark infringement law does not impose on service providers an affirmative duty to seek out infringing content or products posted on the websites they operate, or passing through their networks.[291] For example, in *Tiffany v. eBay*, the Second Circuit held that although eBay was generally aware that its site was being used to sell thousands of counterfeit Tiffany products, this did not support a claim for contributory infringement against eBay.[292] Because eBay took prompt measures to remove specific items reported to be infringing, but did not otherwise have "[c]ontemporary knowledge of which particular listings [were] infringing," eBay

287. 17 U.S.C. § 512 (2006).

288. 17 U.S.C. § 512(b)(2)(E) (2006).

289. *Viacom*, 718 F. Supp. 2d at 525.

290. *Id.* at 526.

291. Tiffany (NJ) Inc. v. eBay Inc., 576 F. Supp. 2d 463, 515 (S.D.N.Y. 2008).

292. Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93, 107 (2d Cir. 2010).

was found to have satisfied its legal obligations.[293] However, if the evidence showed that eBay was "willfully blind" to the infringement – that is, that it "intentionally shielded itself from discovering the offending listings" – a contributory infringement claim could lie.[294]

Opponents argue that PIPA and SOPA threaten to upset the existing balances of the contributory liability doctrine and the DMCA safe harbor provision, shifting the burden to police infringing content from the intellectual property owner to the website host. Thus, sites like YouTube and eBay would be placed in the position of monitoring the vast and constantly evolving bodies of user-generated content that appear on their sites, and making unilateral determinations whether such content might infringe the rights of known or unknown third parties, lest they be shut down or deprived of funding. However, supporters insist that the bills are directed toward "foreign rogue websites," and not intended to impose such draconian measures against legitimate websites.[295] Representative Lamar Smith, SOPA's primary sponsor, contends that blogs and social networking sites "have nothing to worry about."[296] This is because "[w]ebsites like Facebook and YouTube that host user content are not 'primarily dedicated to' illegal activity" and do not market themselves as such.[297] Notwithstanding these assurances, sites like YouTube and eBay may have legitimate cause for concern, as Mr. Smith cannot guarantee that the Attorney General or brand and content owners such as Tiffany and Viacom will agree.[298]

293. *Id.*

294. *Id.* at 109.

295. Edward Wyatt, *Lines Drawn on Antipiracy Bills*, N.Y. TIMES (Dec. 14, 2011), *available at* http://www.nytimes.com/2011/12/15/technology/lines-are-drawn-on-legislation-against-internet-piracy.html?pagewanted=all.

296. U.S. HOUSE OF REPRESENTATIVES JUDICIARY COMMITTEE, MYTH VS. FACT: STOP ONLINE PIRACY ACT, *available at* http://www.judiciary.house.gov/issues/Rogue%20Websites/011812_SOPA%20Myth%20vs%20Fact.pdf (last visited March 19, 2012).

297. *Id.*

298. Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93, 97 (2d Cir. 2010). For example, in its suit against eBay, Tiffany claimed that its own investigations revealed that 73.1% and 75.5% percent of TIFFANY merchandise purchased through eBay in 2004 and 2005 was counterfeit. Tiffany (NJ) Inc. v. eBay Inc., 576 F. Supp. 2d 463, 512 (S.D.N.Y. 2012) (these studies were deemed

2. Compromising the Security and Stability of the Internet

Some of the strongest opposition to PIPA and SOPA pertains to the ability to manipulate the Domain Name System (DNS). In simplest terms, the DNS is a like a telephone directory for the Internet. Computers communicate with each other using numerical IP addresses (for example the IP address for Google.com is 207.151.159.3), which are difficult for humans to remember.[299] In order to make the Internet user-friendly, DNS translates easy-to-remember domain names, such as google.com, into the numerical IP Addresses that computers use to identify locations on the Internet.[300]

As one way to combat online infringement, PIPA and SOPA would allow the Attorney General to obtain an order compelling service providers to block DNS translation of domain names, severing the domain name from its associated IP address. Some opponents argue that DNS filtering would undermine the universality of domain names, "one of the key enablers of the innovation, economic growth, and improvements in communications and information access unleashed by the global Internet."[301]

In addition, DNS filtering is said to raise cybersecurity concerns. Critics contend that the system proposed by PIPA and SOPA, which would include redirecting users to different resources (such as a message from the Department of Justice) in response to a DNS request, is incompatible with DNS Security Extensions (DNSSEC) measures designed to authenticate DNS records.[302] By interfering with, or inhibiting DNSSEC authentication, PIPA and SOPA would potentially threaten cybersecurity with respect to "distribution of malware and other problematic Internet behavior . . . which could expose personal information, credit card data, e-mails, documents, stock data, and other sensitive information."[303] Further still, opponents explain that DNS filtering and re-direction would

"methodologically flawed and of questionable value" by the trial court).

299. CROCKER ET AL, *supra* note 242, at 3.

300. *Id.*

301. *Id.* at 4.

302. *Id.* at 5.

303. *Id.*

threaten security in the absence of a "mechanism to distinguish court-ordered lookup failure from temporary system failure, or even from failure caused by attackers or hostile networks."[304]

Perhaps most compelling are arguments that the bills' DNS filtering and re-direction approach is easily circumvented, and therefore simply ineffective. First, the filtering will not remove any infringing content from the targeted website, or even disable the website. Filtering only severs the tie between the domain name and the IP address where the website resides. Thus, even if DNS filtering blocked translation of the domain google.com, its content would still be accessible if accessed directly by its (numerical) IP address. The websites would also remain accessible through non-filtered nameservers.[305] And of course, the infringing content can also remain accessible through the DNS by the website owner simply moving it to a new domain name.

Faced with strong concerns about the ramifications of PIPA and SOPA on the security and stability of the DNS, the filtering provisions were removed from the bills.[306]

3. Constitutional Concerns

The bills' supporters have taken the position that the "First Amendment is not an excuse for illegal activity."[307] Opponents, however, contend that PIPA and SOPA, by potentially shuttering allegedly infringing websites on an *ex parte* basis, without affording the owner an opportunity to be heard, impose impermissible prior restraints on speech.[308] To avoid unnecessarily infringing critical First Amendment rights,

304. *Id.*

305. *Id.* at 7.

306. Jon Swartz & Scott Martin, *Proposals Spur Website Protests*, USA TODAY (Jan. 17, 2012, 8:50 PM), http://www.usatoday.com/MONEY/usaedition/2012-01-18-SOPA-Protest_ST_U.htm.

307. U.S. HOUSE OF REPRESENTATIVES JUDICIARY COMMITTEE, *supra* note 296.

308. Letter from Mark A Lemley, David S. Levine, and David Post to House of Representatives (Nov. 15, 2011), *available at* https://www.cdt.org/files/pdfs/SOPA_House_letter_with_PROTECT_IP_letter_FINAL.pdf.

allegedly infringing websites should not be shuttered until after a "prompt final judicial determination [on the legality of the conduct] in an adversary hearing."

To the extent that PIPA and SOPA draw upon civil forfeiture procedure, their constitutionality is under collateral attack in *Puerto 80 Projects, S.L.U. v. United States*.[309] *Puerto 80* arose out of the Department of Homeland Security Immigration and Customs Enforcement's (ICE) wave of domain name seizures dubbed "Operation in Our Sites 2.0."[310] ICE obtained a seizure warrant for two of Puerto 80's domain names, rojadirecta.org and rojadirecta.com, which were allegedly used to commit criminal copyright infringements, namely, the streaming of copyrighted broadcasts of sporting events.[311] Puerto 80 challenged the seizure in the District Court for the Southern District of New York and petitioned for return of its domain names, contending that its sites merely hosted message forums and indexed links to – but did not directly host – the infringing content.[312] Puerto 80 also claimed that the seizure and suppression of its website violated its First Amendment rights.[313] The Court denied Puerto 80's petition, finding that the alleged First Amendment violations did not constitute the "substantial hardship" required to release the domains.[314] Puerto 80 appealed to the Second Circuit, arguing that the *ex parte* seizure of the domains constituted a prior

309. *See* Puerto 80 Projects, S.L.U. v. United States, No. 11-3390-cv, 2011 WL 6148823 (2d Cir. Dec 6, 2011).

310. Press Release, Department of Homeland Security Immigration and Customs Enforcement, New York Investigators Seize 10 Websites That Illegally Streamed Copyrighted Sporting and Pay-Per-View Events (Feb. 2, 2011), *available at* http://www.ice.gov/news/releases/1102/110202newyork.htm.

311. *Id.*

312. Petition for Release of Seized Property at ¶ 26, Puerto 80 Projects, S.L.U. v. United States, 1:11-cv-3983-PAC (S.D.N.Y. June 13, 2011), *available at* http://www.citmedialaw.org/sites/citmedialaw.org/files/2011-06-13-Puerto%2080%20Petitionfor%20Release%20of%20Seized%20Property.pdf.

313. *Id.* ¶¶ 20-21.

314. Order Denying Release of Domain Names, at 4, Puerto 80 Projects, S.L.U. v. United States, 1:11-cv-3983-PAC (S.D.N.Y. Aug.4, 2011), *available at* http://www.citmedialaw.org/sites/citmedialaw.org/files/2011-08-04-District%20Court%20Order.pdf.

restraint on speech, rendering the seizures unconstitutional.[315] As of the writing of this article, the Second Circuit has not yet issued its decision, and rojadirecta.org and rojadirecta.com continue to display ICE seizure notices more than a year later.[316]

Opponents of PIPA and SOPA also point out that the bills stand to affect the freedom of expression of individuals beyond that of the infringer.[317] For example, if a blogging site were found to host an infringing post, the Attorney General could conceivably have the entire site shut down, thus suppressing an overwhelming and disproportionate amount of non-infringing speech. In addition to the problems of notice and prior restraints symbolized by the *Puerto 80* case, this type of "collateral damage" to non-infringing speech is a serious cause for concern among free-speech advocates.[318]

V. Conclusion

As the dust starts to settle after the flurry of activity surrounding this legislation, we see that opponents to the bills have passionately outlined the parade of horribles they fear would follow should this legislation (in any of their drafted forms) be approved. Interestingly, proponents of the bills agree that the negative implications raised by the opponents would be important to avoid. However, they argue that the parade of horribles is outside the intent and goals of the bills and unlikely to come to fruition.

For now, we put aside discussion of the merits of the opposition to the proposed legislation. Instead, we consider the impact the proposed legislation would have on the battle

315. Opening Brief of Petitioner-Appellant at 2, Puerto 80 Projects, S.L.U. v. United States, No. 11-3390 (2d Cir. Sept. 16, 2011), *available at* http://www.citmedialaw.org/sites/citmedialaw.org/files/2011-09-16-Puerto%2080%20Opening%20Brief.pdf.

316. *See* ROJADIRECTA, rojadirecta.org (last visited July 25, 2012); ROJADIRECTA, rojadirecta.com (last visited July 25, 2012).

317. Laura W. Murphy & Michael W. Macleod-Ball, *Stop Online Piracy Act, in* WRITTEN STATEMENT OF THE ACLU 2 (2011), *available at* https://www.eff.org/sites/default/files/filenode/Statement%20to%20HJC%20SOPA%2011-16-11.pdf.

318. *Id.*

against counterfeiters if the bills achieve what their supporters argue is their intended purpose We conclude that passage of any of these bills would serve as an endorsement of the efforts that are discussed in this paper, and which are already underway by brand owners, payment processors and the federal government.[319]

In particular, passage of this legislation would send a message to federal courts that permitting brand owners to efficiently and cost-effectively resolve counterfeit disputes involving large numbers of domains is consistent with the goals set by Congress. Likewise, the district courts' orders compelling domain name registrars and payment processors to disable websites and intercept funding for such sites, closely parallels the statutory language of PIPA and SOPA that aim to authorize such action. Moreover, passage of these bills would not only endorse the (now) voluntary actions taken by credit card processors, but would make them mandatory, immunizing the processors for their efforts in assisting brand owners with termination of counterfeit websites, and for policing use of their own marks.

This naturally leads to the questions of: (1) whether the tools available to brand owners that are discussed in this article, namely mass domain lawsuits and assistance of payment processors, which seemingly would be endorsed by SOPA and PIPA, are sufficient to overcome the ever-crippling problem of online counterfeit websites; and (2) given that these tools already exist, whether the passage of SOPA and/or PIPA would have any impact on the effectiveness of these tools. The answer: we don't know – yet.

In the end, it almost certainly comes down to the numbers. For brand owners to prevail, they need to reach a level of efficiency whereby they can manipulate these tools (and perhaps other tools) to create enough of a disruption – in terms

319. A federal government seizure of the popular filing sharing website megaupload.com, and the arrest of four of its owners earlier this year, prompted many to question whether legislation such as SOPA and PIPA are truly necessary. The seizure of megaupload.com highlighted the powers already vested in the federal government to combat online piracy. *See* Andrew Couts, *MegaUpload Shut Down by Feds: Why Do We Need SOPA?*, YAHOO! NEWS (Jan. 19, 2012), http://news.yahoo.com/megaupload-shut-down-feds-why-sopa-225952735.html.

of sheer number of terminated websites, disabled merchant accounts and frozen financial assets – that it no longer remains profitable for a website owner to continue creating and optimizing new sites, registering new domains, and establishing new merchant accounts. Or at minimum, so that the counterfeit website owner is persuaded to simply direct its counterfeit activity towards some other less aggressive brand owner's property.

To date, this threshold has not been reached, by even the most actively-enforcing brand owners. Until this balance is tipped in brand owners' favor, whether by SOPA, PIPA or otherwise, there will be insufficient incentive for the counterfeit website owners to refrain from their present scheme of avoiding eradication through volume and anonymity.