

# Rogues and Registrars

Are some Domain Name Registrars safe havens for Internet drug rings?

a report by LegitScript and Knujon

Canadian Health&Care Mall – Buy cheap online! Buy cheapest Viagra, Cialis, Propecia etc.

http://canadianhealthcaremall.net/

Google

**CANADIAN Health&Care Mall**



Your Cart Items: 0 | Total: \$0.00

USD CAD EUR GBP AUD CHF

**MEN'S HEALTH**

best sell

**Cialis + Viagra Powerpack**

**Viagra**

**Viagra Super Active+**

**Viagra Professional**



**MINNESOTA BOARD OF PHARMACY**

link to a "Drug Reselling License" purp  
"licenses" are enclosed with this letter).

censes" mentioned above are forgeries,  
s a "rogue Internet pharmacy" operating

## executive summary

The Internet is sometimes said to be the “Wild West” — a place without any rules. The sentiment is understandable, but incorrect: the Internet *does* have rules. These rules are supposed to ensure the growth of the Internet in a way that fosters legitimate personal and commercial activity, but prevents an out-of-control explosion of fraud and crime.

In this report, we examine how Domain Name Registrars — companies that are supposed to follow those rules — responded when put to the test. From November 2009 through April 2010, the authors provided evidence to over a dozen Domain Name Registrars establishing that each company’s paid domain name registration services were being used by one or more Internet drug rings to register websites engaged in criminal and fraudulent activity. The authors then asked the Registrars to enforce their own Terms and Conditions regarding each website.

The Internet rule that is most pertinent to this report is straightforward. Domain Name Registrars — companies like GoDaddy, Network Solutions, eNom and others who register domain names — are required by ICANN, the organization that accredits (and can de-accredit) them, to prohibit website owners from using their domains for unlawful purposes. Without exception, this rule is also reflected in each Registrar’s Terms and Conditions, thus formalizing and protecting the company’s contractual right to suspend domain names for unlawful activity. Once a Registrar becomes aware that a website is engaged in criminal activity, the company has the legal authority and technical ability to suspend the domain name, rendering the illegal and fraudulent content inaccessible. This self-policing is meant to balance freedom of speech with safety and legitimacy as the Internet continues to evolve.

But all too often, Registrars simply turn a blind eye to criminal activity. After all, Registrars have an inherent financial conflict of interest: on the one hand, they are supposed to adhere to the policy requiring them to prohibit unlawful activity; on the other hand, they stay in business from the registration and re-registration fees that website owners pay to keep those very websites online. As for-profit companies, Registrars will readily shut down a website that fails to pay annual re-registration fees. But as we show, not all Registrars will suspend a domain name if presented with irrefutable evidence that the customer is using the website to commit fraud or a crime.

To document this, the authors provided indisputable evidence to these Domain Name Registrars that websites were displaying a forged pharmacy license and/or selling drugs without requiring a prescription. Our evidence included letters from the government agencies that license pharmacies stating that the pharmacy “license” displayed on the website’s home page was a forgery. In other cases, the website clearly and overtly advertised prescription drugs such as Vicodin, Viagra or OxyContin “without a prescription.”

Additionally, most of the US-based Registrars identified in this report had, in late 2008, received a letter from the National Association of Boards of Pharmacy (NABP) informing them that the NABP had recognized LegitScript’s standards for Internet pharmacy verification, and asking those Registrars to work with LegitScript to identify “rogue” Internet pharmacies misusing those companies’ domain name registration services. The intent of these letters was to request that the Registrars give credence to LegitScript’s notifications, based on the NABP’s recognition of LegitScript’s program, and the NABP’s own status as the organization that represents pharmacy-related regulatory authorities.

The good news is, most of the Registrars we contacted acted to prevent the further use of their services by websites engaged in illegal or fraudulent activity. Part of the reason for this report is to recognize and applaud the actions taken by those Registrars, including GoDaddy, Directi, SpiritDomain, and several others.

However, a handful of Registrars — three in the United States (eNom, UK2Group and Moniker), one in Russia (CentroHost) and one in the Netherlands (Realtime Register) — after being notified about the criminal behavior in question, declined or even refused to take steps to prevent the continued use of their registration services by these websites. In some cases, it appears that they even permitted re-registration of the websites' domain names.

In their responses to us, the most common refrain we heard from the Registrars that elected to allow these websites to continue using their registration services was that the company is “only the Registrar” and, even if they receive information that their registration services are being used in the furtherance of criminal or fraudulent activity, will not do anything without a court order.

Beyond mere common sense, there are four primary reasons that the Registrars could (and should) have terminated their relationship with these illicit websites. First, as a matter of law, individuals or companies who become aware that they, or something in their control, are being used to facilitate criminal or fraudulent activity, but do nothing about it, may themselves be held responsible, especially if a financial relationship exists between the parties (e.g., Registrar and registrant). Second, as we explain, it is precisely because these companies are Registrars, not in spite of it, that they are bound to act once put on notice, not turn a blind eye to criminal activity. Third, due to the “jurisdiction-less” nature of the Internet itself, Registrars should know that in many cases, a court order is an impossibility — a fact that cyber-criminals count on. Fourth, as we show, several Registrars did move to stop their domain name registration services from being used in furtherance of unlawful activity. It is therefore reasonable to ask companies like eNom, UK2Group and Moniker to explain why they, unlike GoDaddy, SpiritDomains and Directi, chose to allow the continuing use of their domain name registration services by websites engaged in crime or fraud.

In this report, we also take ICANN to task for what the authors view as inattention to, or nonchalance regarding, this issue. ICANN is the accrediting institution for Domain Name Registrars. If accreditation by ICANN is to mean anything, ICANN must take its role as an accrediting institution seriously, and must insist that Registrars adhere to its policies and rules.

Why is this important? Among other reasons, in the way that we use the Internet today, domain names are at the core of how the Internet is organized, accessed and understood. For most Internet users, there is no distinction between a website and a domain name.<sup>1</sup> Consequently, how the sale, transfer and suspension of domain names occurs will determine the future integrity of the Internet. This implicates Domain Name Registrars, and highlights the responsibility that they have — and that ICANN, their accrediting institution has — to ensure some semblance of order and accountability. Like any website owner, Internet criminals rely upon domain name registration services to reach their customers. Turn off the criminals' access to the domain name registration service, and the opportunity for criminals to make victims out of Internet users is disrupted.

The authors invite the Registrars who elected to allow the continued use of their registration services by illicit websites — eNom, UK2Group, Realtime Register, CentroHost and Moniker — to engage in a public discussion regarding their responsibilities as ICANN-accredited Registrars. More specifically, the authors call on these Registrars to explain why, after being put on notice that their paid registration services are being used by websites easily verified as engaging in criminal and fraudulent activity, including the display of fake pharmacy licenses and/or the sale of prescription drugs without a prescription, the websites are still online; the domain names are still sponsored by these companies; and these companies are continuing to allow the websites to still use their domain name registration services.

---

<sup>1</sup> Technically, a website's content does not exist “at” a domain name, but rather on a server, usually with an IP address (e.g., 82.52.83.255), and the domain name “points” to the IP address. But that is precisely the point: the world uses the Internet by inputting domain names into browsers, not IP addresses. Consequently, the domain name is just as integral of a part of the website as the IP address and content.

## table of contents

- I. the rules of the Internet (and who has to play by them)
  - A. the Internet: not really the wild west
  - B. the Uniform Dispute Resolution Policy — not just about trademarks
  
- II. evapharmacy: the world's largest Internet drug ring
  
- III. eleven Registrars that made the Internet safer...
  - 1. GoDaddy (United States)
  - 2. Directi (India)
  - 3. Advantage-Interactive (United Kingdom)
  - 4. Spirit Domains (United States)
  - 5. Joker (Germany)
  - 6. Web Werks (India)
  - 7. BizCN.com (China)
  - 8. Network Solutions (United States)
  - 9. Visesh / SignDomains (India)
  - 10. Sibername (Canada)
  - 11. AZ.pl (Poland)
  
- IV. ...and five that left the websites online
  - 1. eNom (United States)
  - 2. CentroHost (Russia)
  - 3. Realtime Register (Netherlands)
  - 4. UK2Group (Gibraltar/United States)
  - 5. Moniker (United States)
  
- V. ten common Registrar excuses dissected
  
- VI. conclusion

**Disclaimer.** LegitScript and KnujOn are independent companies wholly owned by their respective staff. This report was not prepared for or at the request or suggestion of any third party, including but not limited to any domain name registrar, Internet service provider, government agency, pharmacy or pharmaceutical manufacturer.

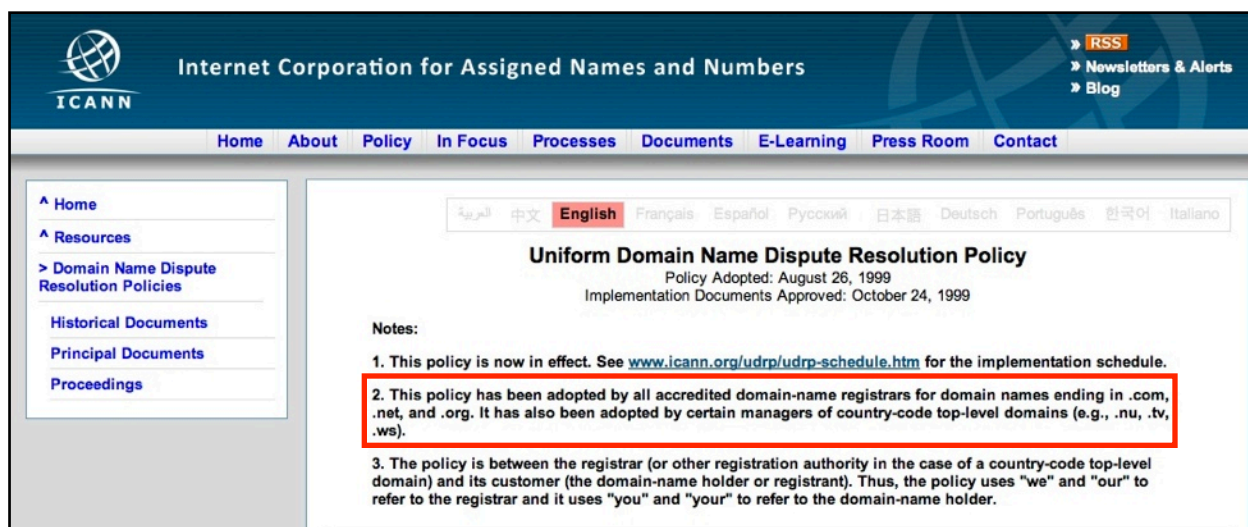
# 1 the rules of the Internet (and who has to play by them)

Does the Internet really have rules — and what are they?

The body that accredits Domain Name Registrars (companies such as GoDaddy or Network Solutions) and gives them permission to register domain names<sup>2</sup> is called the Internet Corporation for Assigned Names and Numbers (ICANN). When a company becomes accredited to register domain names, it is then bound to follow certain policies and contractual requirements.

One of these rules is a policy called the Uniform Dispute Resolution Policy (UDRP). The UDRP provides a contractual model for the Terms and Conditions that must exist between a Domain Name Registrar and its customers (domain name registrants). On its website, ICANN states:

**All Registrars must follow the the Uniform Domain-Name Dispute-Resolution Policy (often referred to as the "UDRP").**



The screenshot shows the ICANN website's page for the Uniform Domain Name Dispute Resolution Policy. The page header includes the ICANN logo and navigation links. The main content area features the title 'Uniform Domain Name Dispute Resolution Policy' and a list of notes. Note 2 is highlighted with a red box, stating: '2. This policy has been adopted by all accredited domain-name registrars for domain names ending in .com, .net, and .org. It has also been adopted by certain managers of country-code top-level domains (e.g., .nu, .tv, .ws).'

All Domain Name Registrars accredited by ICANN must adhere to the Uniform Dispute Resolution Policy. The UDRP includes a requirement that domain name registrants not knowingly use the domain name in violation of any applicable laws or regulations, yet several Domain Name Registrars seem to ignore this requirement.

The UDRP deals mostly with trademark disputes and cybersquatting, but it also deals with unlawful activity. In some form or another, each Registrars' Terms and Conditions must require this of its customers:

**Your Representations**. By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that...**(c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations** (emphasis added).<sup>3</sup>

The UDRP is clear: accredited Registrars must prohibit their customers (domain name registrants) from using websites for unlawful purposes.

<sup>2</sup> Our discussion here only focuses on .com, .net, .org and other commonly used domain names. There are separate processes for many "county code" top level domains, such as .jp for Japan, or regional ones like .eu for Europe. As a practical matter, most of these also require adherence to the same or similar rules as we describe.

<sup>3</sup> <http://www.icann.org/en/udrp/udrp-policy-24oct99.htm>

**As we show, some Registrars responded to us as if this requirement does not exist.**

Indeed, in some cases, it seemed as if the Registrar believed that Registrars need not do anything even when provided clear and incontrovertible evidence that their services are being used in the furtherance of criminal activity. Some Registrars, such as UK2Group, specifically responded to us that the UDRP only deals with trademark issues, and imposes no requirements related to unlawful activity. Clearly, this is incorrect, given the plain language of the policy above. A possible reason for this mistake is that most of the UDRP does address trademark disputes, and a process has been set up — commonly referred to as the UDRP or UDRP process — to navigate trademark disagreements. However, the language of the UDRP itself is absolutely clear: domain name registrants must agree not to register or use the domain name for an unlawful purpose, and ICANN-accredited Registrars are bound by this policy requirement.

All ICANN-accredited Domain Name Registrars' Terms and Conditions thus contain some variant<sup>4</sup> of the above language, prohibiting use of the domain name for unlawful purposes, and giving Registrars the right to suspend the domain name if illegal activity is found. Importantly for this report, ICANN does not require (and neither do any Registrars) a court order or judicial finding, which — for reasons we explain more fully in this report — would be an impossibility to provide in many cases due to the jurisdiction-less nature of the Internet itself.

---

<sup>4</sup> For example, GoDaddy's Terms and Conditions state: **NO UNLAWFUL CONDUCT OR IMPROPER USE.** As a condition of Your use of Go Daddy's Services, You agree not to use them for any purpose that is unlawful...Go Daddy may also cancel Your use of the Services if You are using the Services, as determined by Go Daddy in its sole discretion, in association with...activities prohibited by the laws of the United States and/or foreign territories in which You conduct business...

## 2 Internet drug rings and forged pharmacy licenses

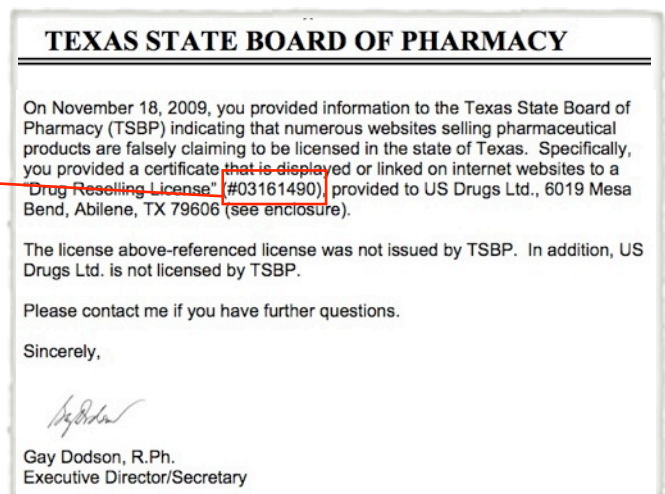
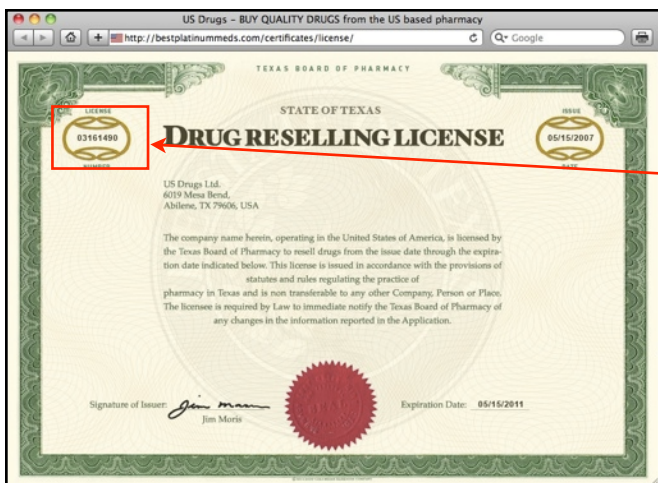
**Among the most prevalent types of Internet crime** are “rogue Internet pharmacies” — websites that claim to be safe or authentic sources of prescription drugs, but are typically not pharmacies at all, and actually engage in a variety of dangerous, deceptive, and criminal acts.

Rogue Internet pharmacies often operate as networks, or Internet drug rings, comprised of hundreds or thousands of websites. These websites typically engage in four main types of illegal activity: 1) the sale of unapproved or counterfeit drugs; 2) not requiring a prescription for prescription drugs; 3) the lack of an appropriate pharmacy license; and 4) consumer or patient fraud. The dangers can range from receiving fake drugs; getting sub-standard or addictive medicines without a prescription; or even identity theft.

One of the world’s largest Internet drug rings is called **EvaPharmacy**.<sup>5</sup> The organization is a shadowy network that claims to be based in the US and Canada, but is run largely out of Russia. At its height, about six months ago, the network operated close to 8,500 websites that claimed to be pharmacies, going so far as to display seemingly real pharmacy licenses from Minnesota, Texas, Manitoba, Ontario or Quebec on their websites. Today, EvaPharmacy continues to operate about 2,000 websites, but has shrunk in size, we believe, due to the response of some Registrars listed in this report.



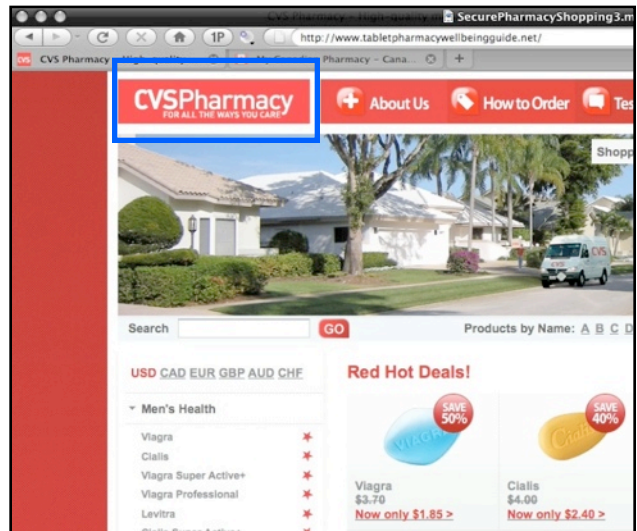
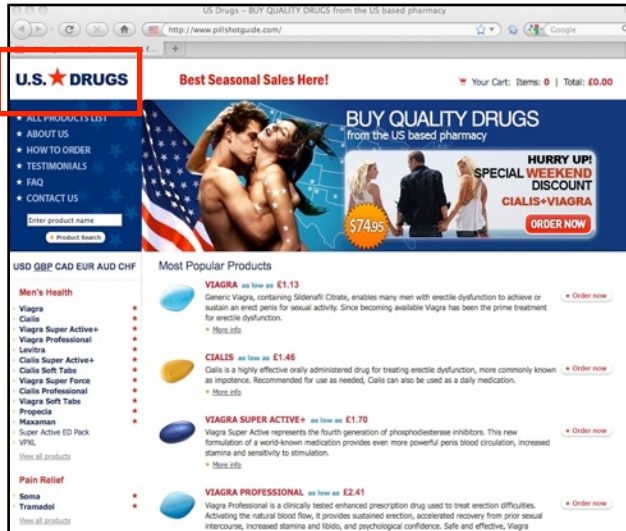
Drugs purchased from [CanadianHealthCareMall.net](http://CanadianHealthCareMall.net), registered with eNom. We gave eNom a statement by a government agency that the website’s “Minnesota pharmacy license” is a forgery. The drugs arrived from India without a prescription. eNom has still not suspended the website’s domain name.



A fake pharmacy license displayed at [bestplatinummeds.com](http://bestplatinummeds.com); to the right is the letter from the Texas agency that licenses pharmacists attesting that the license is a forgery. UK2Group received this notification, but the website is still online.

<sup>5</sup> Over the last two to three years, an organization known as GlavMed (connected to EvaPharmacy) has tended to have the most affiliate websites. For several months in 2009, EvaPharmacy overtook GlavMed, according to LegitScript’s monitoring.

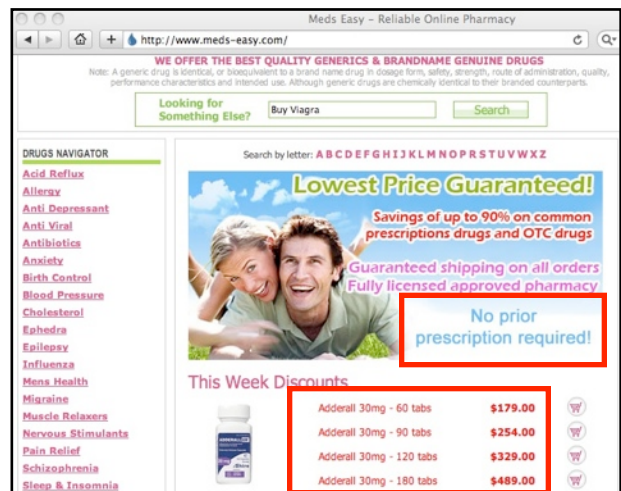
The rogue Internet pharmacies that make up the EvaPharmacy Internet drug ring are built on lies and crime: deliberately misleading potential customers, the pharmacy licenses are forgeries — blatant fakes. Some even market themselves as “CVS Pharmacy”, a well-known chain drug store. To compound that, none of the websites require a prescription; all of them sell fake or banned drugs; and all illegally import prescription drugs from offshore locations such as India — a hotspot for counterfeit medications.



The EvaPharmacy Internet drug ring displays a fake US or Canadian pharmacy license and urges Internet users to “Buy Quality Drugs from the US-based pharmacy” or refers to itself as “CVS Pharmacy”, duping Internet users into believing that they are ordering from a well-known chain drugstore in the United States.

To remove any reasonable doubt about the fraudulent and illegal nature of some of these websites, LegitScript and KnujOn approached the Boards of Pharmacy<sup>6</sup> in the states and provinces where these websites claim to be licensed. The Boards of Pharmacy are government agencies responsible for licensing pharmacies and pharmacists. Each of the five Boards of Pharmacy provided us with a letter stating that the “pharmacy license” displayed on the websites’ home page was a forgery (see attached letters). As explained below, these letters were provided to all Registrars whose registration services had been used for such websites.

Although the forged nature of the pharmacy license is one clear indicator of illegal activity, other illegal Internet pharmacies did not display a fake (or any) pharmacy license, but were nevertheless clear in offering prescription drugs without a prescription, or could easily be verified as acting unlawfully in



We notified Moniker twice about meds-easy.com, which sells drugs like Vicodin and OxyContin without a prior prescription, in direct violation of the Controlled Substances Act. The website remains open for business.

<sup>6</sup> In Canada, these are referred to as Colleges of Pharmacy, and are responsible for licensing pharmacists and pharmacy/pharmacist oversight in general.



other ways. The authors clearly documented the illegal activity of those websites with screenshots and other evidence. For example, the authors have notified Moniker about the website [meds-easy.com](http://meds-easy.com), which offers OxyContin without a valid prescription, on two separate occasions. That website can easily be verified as selling Vicodin, an addictive controlled substance prescription medication, without requiring a prescription. The website is still doing business online, and Moniker remains its sponsoring Domain Name Registrar.

In summary, the authors acquired and provided each Registrar with evidence that was clear and well-documented, and for the US-based Registrars, the evidence was provided via certified US Mail and, in some cases, on multiple occasions.

So how did the Registrars respond? As we show, several Registrars, both in the US and elsewhere, responded quickly and appropriately — but some allowed the illegal websites to survive and thrive.

### 3 eleven Registrars that made the Internet safer

First, the good news. **Eleven Domain Name Registrars acted — in most cases, fairly swiftly — to ensure that their registration services were not being used in the furtherance of criminal activity.** The authors note that even though most of our complaints were based on violations of US law, these Domain Name Registrars are located around the world.

- **SpiritDomains**, in the United States, within minutes, shut down 180 websites that were selling drugs without a prescription and posting fake pharmacy licenses.
- **Directi**, in India, has shut down over 5,000 rogue Internet pharmacies, including those engaged in the sale of counterfeit drugs, based upon our notifications.
- **GoDaddy**, in the United States, has disabled more than 3,500 “rogue Internet pharmacies” following our notifications, based on the websites’ offering prescription drugs without a prescription.
- **Advantage-Interactive**, in the United Kingdom, shut down the 46 fake Internet pharmacies we notified the company about.
- **Joker**, in Germany, disabled 263 rogue Internet pharmacies upon receiving notification.
- **BizCN.com**, in China, disabled 104 rogue Internet pharmacies selling prescription drugs without a prescription, and displayed forged pharmacy licenses.
- **Network Solutions**, in the United States, eventually complied with our notifications, after several months and repeated requests, suspending 309 domain names.
- **Web Werks**, in India, suspended 71 domain names for rogue Internet pharmacies.
- **SignDomains (aka Visesh)**, in India, suspended 325 domain names for rogue Internet pharmacies.
- **Sibername**, in Canada, suspended three key rogue Internet pharmacies.
- **AZ.pl**, in Poland, suspended two key rogue Internet pharmacies.

Among the Registrars listed above, Directi, GoDaddy, and Spirit Domains deserve particular recognition for their swift response. GoDaddy and Directi have additionally shown important leadership on this issue.

This part of the report is fairly short, because for the most part, the system worked as it was intended to. For example, in notifying GoDaddy about the websites, the company conducted an independent review, and based on the evidence, acted in accordance with its own Terms and Conditions. Some companies, such as AZ.pl, had some questions, and others took longer, but in the end, the process was straightforward: the companies reviewed the abuse allegations, made a reasonable effort to conduct an independent inquiry as to the violation of their Terms and Conditions, and suspended the domain names.

It is worth noting that although all Registrars, either by reference to the UDRP or via inclusion of their own language, prohibit the use of a domain name for unlawful purposes in their Terms and Conditions (although not all enforce this requirement), a few Registrars have gone a step further, explicitly

prohibiting unlawful activity involving the sale of drugs, including pharmaceuticals.<sup>7</sup> However, explicit language related to prescription drugs is not required in order for a Registrar to take action: after all, the sale of prescription drugs without a valid prescription, or of drugs that are not FDA-approved (or, in Canada, approved by Health Canada, et cetera), is typically a criminal offense, so the general prohibition against unlawful activity is sufficient. Indeed, most of the Registrars who took action do not include in their Terms and Conditions a specific prohibition against illegal pharmaceutical sales.

The authors applaud the Domain Name Registrars listed above who refused to let their domain name registration services be used in the furtherance of crime or fraud. But what about the others?

---

<sup>7</sup> GoDaddy: You will not use this Site or the Services found at this Site in a manner (as determined by Go Daddy in its sole and absolute discretion) that...(i)s illegal, or promotes or encourages illegal activity...(or) promotes, encourages or engages in the sale or distribution of prescription medication without a valid prescription...

Spirit Domains: Customer...shall not use or permit use of the (services), directly or indirectly, in violation of any federal, state or local rule, regulation or law, or for any unlawful purpose... including...illegal pharmaceutical distribution...

## 4 ...and five Registrars that left the websites online

By contrast, five Registrars declined to prevent the continuing use of their registration services by some or all of the websites we notified them about. Three of the Registrars are in the United States: eNom (Washington State), UK2Group (Utah) and Moniker (Florida/California/Oregon). One, Realtime Register, is in the Netherlands, and CentroHost is in Russia.

This section of our report is longer and more detailed, and aims to adequately document our notifications to these Registrars and their responses. To begin this discussion, the authors think it is important to quote from each Registrar's Terms and Conditions (in order to clearly show that they have the contractual right to suspend websites engaged in illegal activity) and the information we gave to the Registrar (to show that it was clear, convincing and compelling).

After that, this report dissects the responses provided by four of these five<sup>8</sup> Registrars: after all, if the authors are wrong — if it is correct that Registrars cannot suspend even a clearly illegal website without a court order (as eNom indicated); that the appropriate company to complain to is the ISP, not the Registrar (as eNom and UK2Group suggested); that only the law where the Registrar is physically located is applicable (as CentroHost and a reseller for UK2Group insisted); or that Registrars cannot be expected to determine what is illegal and what is not (as eNom also indicated) — then our report is misplaced.

But as the authors explain, none of those reasons survive scrutiny. We begin with eNom, a Washington-state-based subsidiary of Demand Media. According to LegitScript's database, eNom is the Domain Name Registrar for over 3,000 rogue Internet pharmacies — more than any other Registrar worldwide.

---

<sup>8</sup> Moniker did not provide us with any explanation or response.

## eNom (Demand Media subsidiary)

Headquartered in Bellevue, Washington, eNom is a subsidiary of Demand Media, located in California. eNom is the second-largest Domain Name Registrar in the world, sponsoring just about 9% - 10% of the world's domain names, second only to GoDaddy.<sup>9</sup>



Yet eNom is, according to LegitScript's database, the world's leading sponsoring Registrar of domain names used by rogue Internet pharmacies. Over the last two years, on multiple occasions, the authors have notified eNom about specific Internet pharmacies that utilize the company's domain name registration services. Additionally, the National Association of Boards of Pharmacy (NABP), whose members are the government agencies that regulate and license pharmacies, wrote a letter to eNom, requesting that they suspend websites using eNom's domain name registration services engaged in the illegal sale of prescription drugs. This letter specifically requested that eNom accept notifications about such websites from LegitScript, one of the authors of this report. To the best of our knowledge, eNom has not suspended any of these websites based on these notifications or requests.<sup>10</sup>

### eNom Terms and Conditions

Could eNom suspend the domain names of websites engaged in illegal activity if it wanted to? Yes: eNom's Terms and Conditions give the company the contractual right to suspend domain names for illegal activity:

We...may terminate or suspend the Services at any time for cause, which, without limitation, includes...(iv) allegations of illegal conduct,...or (vii) if your use of the Services involves us in a violation of any third party's rights or acceptable use policies. (Paragraph 5.)

You are bound by all ICANN consensus policies and all policies of any relevant registry, including but not limited to the Uniform Domain Name Dispute Resolution Policy ("UDRP"), which is available at <http://www.icann.org/udrp/udrp-rules-24oct99.htm> and <http://www.icann.org/dndr/udrp/policy.htm> along with the UDRP Rules and all Supplemental Rules of any UDRP provider. (Paragraph 16.)

However, as we show, the company declined to enforce this section of its Terms and Conditions.

### December 1, 2009 and January 21, 2010 notifications

Between December 2009 and January 2010, LegitScript provided notice to eNom, via certified US Mail and email correspondence, regarding over 500 illicit Internet pharmacies. Several of these, such as [canadianhealthcaremall.net](http://canadianhealthcaremall.net) and [cheap-pharmacy.us](http://cheap-pharmacy.us), posted a fake pharmacy license on its home page, and were included in both notifications.

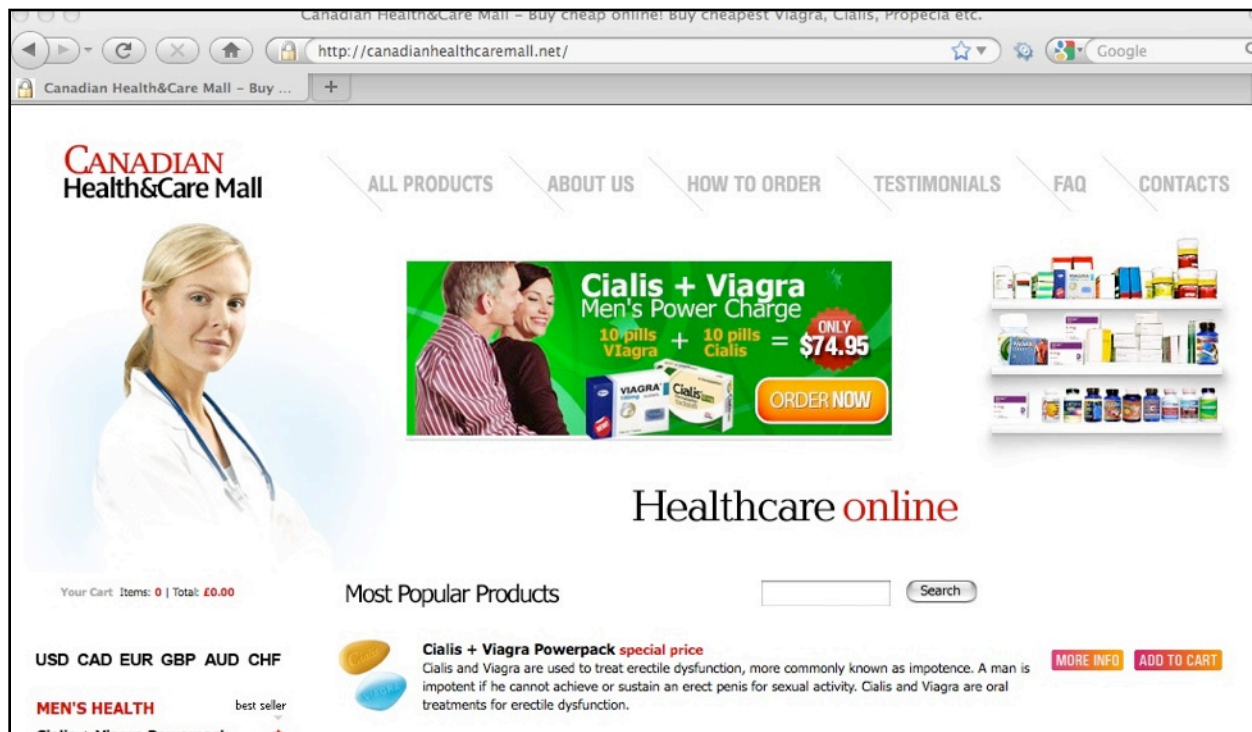
The website [canadianhealthcaremall.net](http://canadianhealthcaremall.net) is one of the EvaPharmacy Internet drug ring's flagship websites; its image is presented on the next page. The website is designed to convince Internet users that it is linked to a *bona fide* Canadian pharmacy. The inclusion of what at first appears to be a

---

<sup>9</sup> See registrarstats.com, accessed 4/30/2010.

<sup>10</sup> Some of the domain names are no longer active, but our research indicates that it is for one of three reasons: 1) natural expiration of the registration; 2) non-payment, or 3) spam, denoted by a name server that includes "BlockedforSpam" in the nameserver's name. As we discuss later in this document, most or all Registrars suspend domain names engaged in spam, but suspending a domain name for involvement in spam is not the same as suspending it for illegal pharmaceutical activity, which is the subject of this report.

Minnesota pharmacy license<sup>11</sup>, linked to from the website's home page, additionally implies the legitimacy of this Internet pharmacy.



However, as we explained to eNom in our email:

These websites operate illegally by virtue of selling prescription drugs without requiring a valid prescription, not being licensed in the jurisdictions where they dispense prescription drugs, illegally importing prescription drugs into the countries where the drugs are dispensed, and selling fake drugs such as "female Viagra."

From the authors' perspective, it is not possible that this could have been more clear. Our letter contained screenshots from these websites, showing how to submit a prescription drug order without a prescription (indeed, many of the websites overtly stated "No prescription required"), how the websites specifically stated that the drugs would be imported from locations such as India; and other evidence of criminal activity.<sup>12</sup>

Perhaps the most vivid evidence of criminality is that the website's "pharmacy license" is a forgery. As we explained in our letter and email to eNom:

...consider the pharmacy license listed at canadianhealthcaremall.net, which purports to be either a Minnesota pharmacy license, 02724941.

<sup>11</sup> Putting aside the fact that Minnesota obviously is not in Canada, the point is the same: the website attempts to convey a sense of legitimacy by purporting to be licensed in the US and/or physically present in Canada.

<sup>12</sup> Here, it is important to explain that many rogue Internet pharmacies allow a customer to simply fill out a form without ever seeing a doctor, but often claim that a doctor will review the form. There are extremely limited and tightly controlled occasions in which this is permitted under the law, but none of the exceptions apply here. In the vast majority of cases, including with this Internet drug ring, there is no doctor involved at all. Indeed, the authors conducted test buy from this very website. We received prescription drugs, which (illegally) were shipped from India, without ever being required to see, speak to, or consult with a physician.

(The website states it is licensed in Minnesota but then displays a fake Ontario pharmacy license). This is a forgery. There is no such licensed pharmacy. Please see the attached letters from the Minnesota State Board of Pharmacy confirming this.

To help explain this, we attached images of the pharmacy license, along with the letter from the Minnesota State Board of Pharmacy stating that the license displayed on these websites were forgeries (see images below).

Although lengthy, it is worth quoting in detail from the Minnesota State Board of Pharmacy's letter, a copy of which was sent, both via email and certified US mail, to eNom:



We notified eNom that cheap-pharmacy.us was displaying a fake license, and sent them a letter from the Minnesota Board of Pharmacy. The website is still using eNom's domain name registration service.

The Minnesota Board of Pharmacy is the government agency that is exclusively responsible for licensing and regulating pharmacists and pharmacies for the State of Minnesota... (i)t has come to our attention that a significant number, possibly thousands, of websites selling pharmaceutical products are falsely claiming to be licensed in the State of Minnesota. Specifically, these Internet pharmacies display or link to a "Drug Reselling License" purportedly issued by the Board.

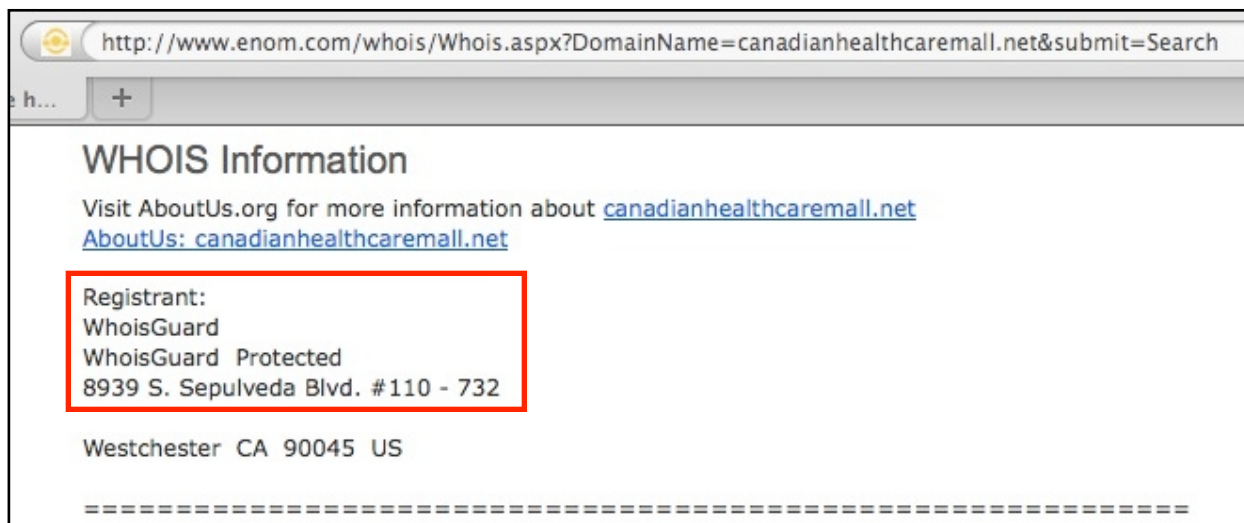
The purpose of this letter is to confirm that the "licenses" mentioned above are forgeries, and any website displaying the above-referenced license is a "rogue Internet pharmacy" operating in violation of the law. The Minnesota State Board of Pharmacy has never licensed any such pharmacy, nor issued any such license number.

**Accordingly, the Minnesota State Board of Pharmacy encourages Domain Name Registrars... to suspend these websites in accordance with their own Terms and Conditions, as well as with ICANN's Uniform Dispute Resolution Policy, Paragraph 2** (emphasis in the original).

On numerous occasions, the Minnesota State Board of Pharmacy has received complaints about the websites that display these licenses. None of the websites require a valid prescription for the sale of prescription drugs, which is unlawful and unsafe. Furthermore, the websites lists pharmaceutical products that are unapproved for sale, that may be counterfeit, and that are potentially dangerous to human health. Many of the complainants have indicated that they received no drug at all, even though their credit cards had been billed.

The websites in the EvaPharmacy Internet drug ring do not merely forge Minnesota state pharmacy licenses, but also licenses purportedly from Quebec, Manitoba, Ontario and Texas. The authors obtained similar or identical letters from those jurisdictions' pharmacy licensing authorities, and presented them to eNom as well for websites displaying fake licenses from those states.

But who actually operates [canadianhealthcaremall.net](http://canadianhealthcaremall.net) — after all, aren't they, not eNom, directly responsible for the content? Yes, but this illuminates another service that eNom provides to the website: an anonymous (“proxy”) domain name registration service that allows the criminal to shield his or her identity. To explain this, ICANN requires every website registrant to submit accurate information about their name, address and email when registering a website. Several Registrars, including GoDaddy and eNom, offer an anonymous service so that this information can be hidden from the public. In eNom's case, this is called “WhoisGuard,” and replaces the website's registration information with a generic one provided by eNom.



eNom also offers a service called “WhoisGuard” that allows domain name registrants to shield their identity from the public. In this case, the owner of [canadianhealthcaremall.net](http://canadianhealthcaremall.net) is using eNom's anonymous service to hide their identity.

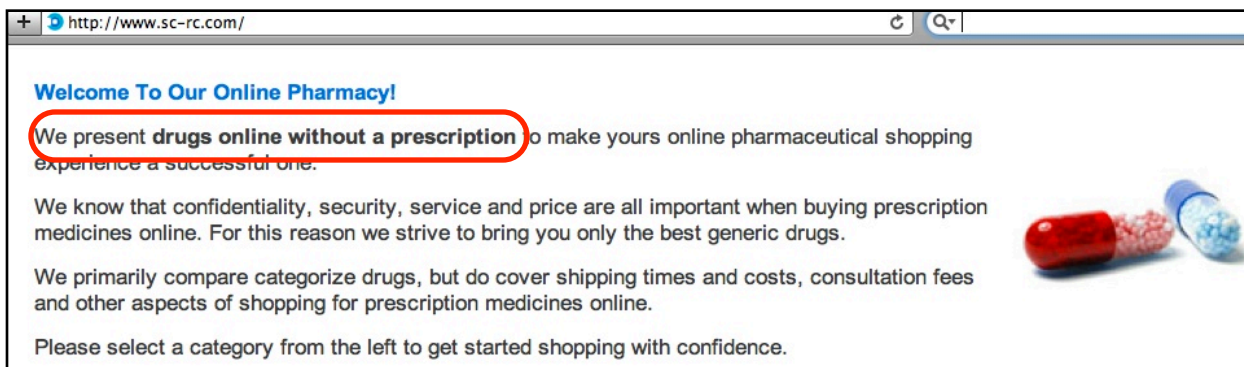
There is nothing inherently wrong with anonymous domain name registration services for individuals — for example, a family who maintains a website with a personal blog or family photos and who may wish to keep their address and phone number private. However, an obvious use of anonymous domain name registration information is also to hide the identities of criminals. In this case, the operator of [canadianhealthcaremall.net](http://canadianhealthcaremall.net) is able to keep his or her identity hidden from the public by the use of eNom's anonymous registration service, conveniently making it impossible to contact him or her with questions about the website.

#### **Other Rogue Internet pharmacies (without a fake license)**

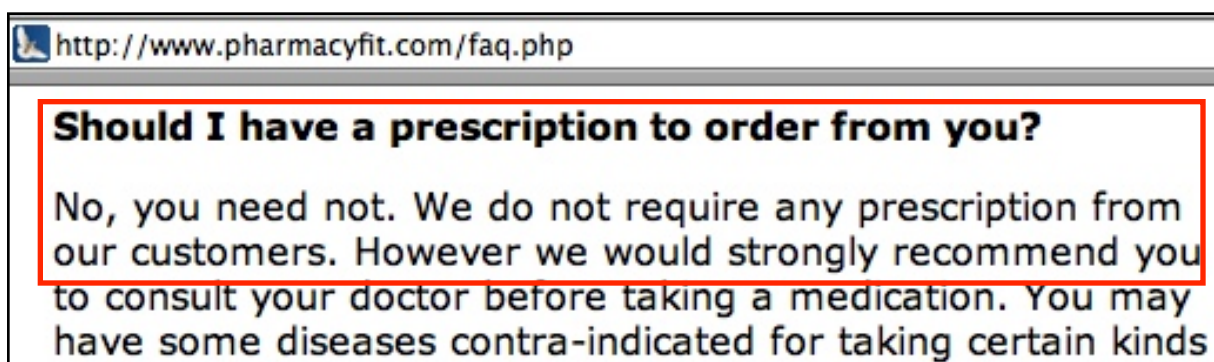
While not all of the rogue Internet pharmacies we notified eNom about displayed fake pharmacy licenses, they were engaged in similarly obvious criminal behavior. Indeed, our December 1, 2009 letter was 48 pages long, addressed to the company's Abuse Department, and contained screenshots regarding over 500 websites that could easily be verified as operating unlawfully.

Consider a few examples below. In our December 1, 2009 report, we included a screenshot of the website [sc-rc.com](http://sc-rc.com), which was (and still is) registered with eNom. The website clearly states that it does not require a prescription for the sale of prescription drugs. The website also utilizes eNom's anonymous website registration service, so that the website owner is able to hide his or her identity.

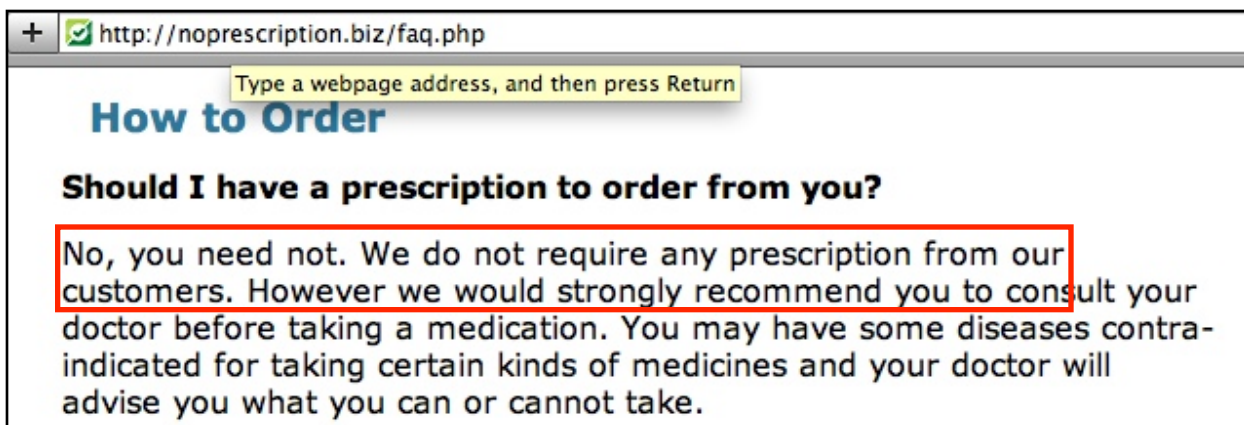
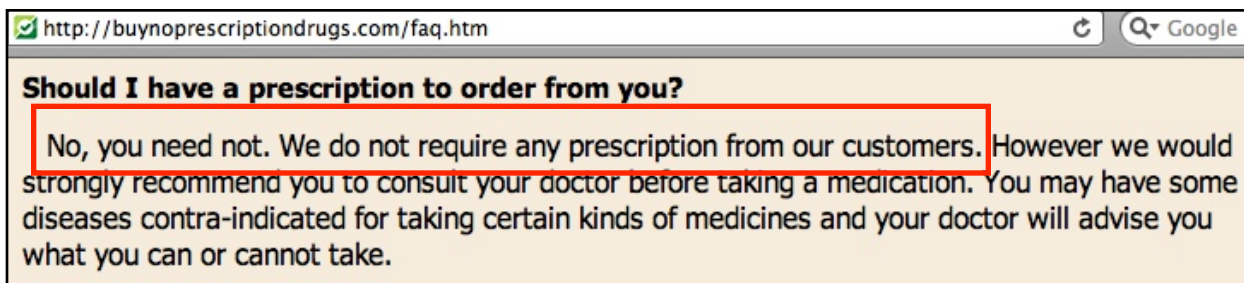




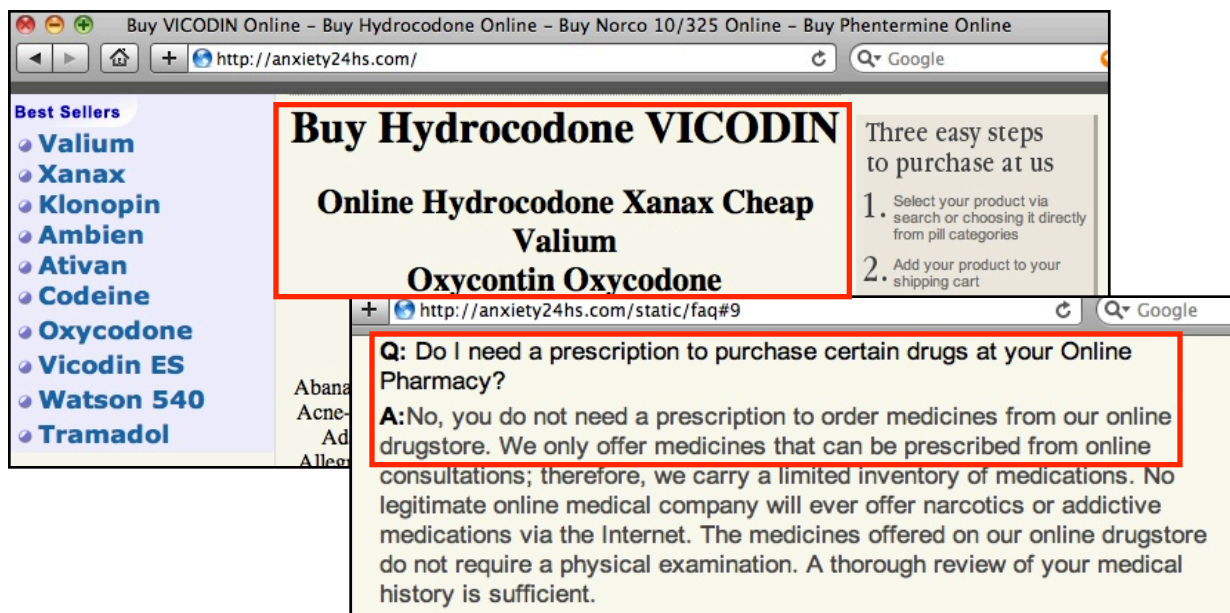
In a similar example, our letter included a screenshot from the website [pharmacyfit.com](http://pharmacyfit.com), which clearly states that it does not require a prescription. As of the writing of this report, the website is still active and registered with eNom — and is likewise using the company’s anonymous website registration service so that the website owner can hide his or her identity from the public.



Among the more than 500 websites we notified eNom about were [noprescriptionpharmacy.biz](http://noprescriptionpharmacy.biz) and [buynoprescriptiondrugs.com](http://buynoprescriptiondrugs.com), which are equally clear: no prescription is required for the sale or purchase of prescription drugs. Both domain names are registered with eNom.



It is also important to note that our notifications included websites selling controlled substances (meaning, prescription drugs that are subject to abuse and addiction, like OxyContin, Vicodin or Xanax). For example, the screenshots below are from [anxiety24hs.com](http://anxiety24hs.com), which sells Valium, a controlled substance, and clearly states that it does not require a prescription. It also sells Xanax, Klonopin, Ambien, Ativan, Codeine and Vicodin, all addictive medications, without a prescription.



In addition to the type of information presented above, our notifications included statements clearly visible on the websites that the drugs would be imported from outside of the country; we explained that this is a violation of federal and many state laws, and cited the laws. We also explained that some of the websites were selling products that had been banned for safety reasons, such as Acomplia, and fake or non-existent products like "Female Viagra," which is also a criminal offense under the US Food, Drug and Cosmetic Act.

#### December 4, 2008 notification

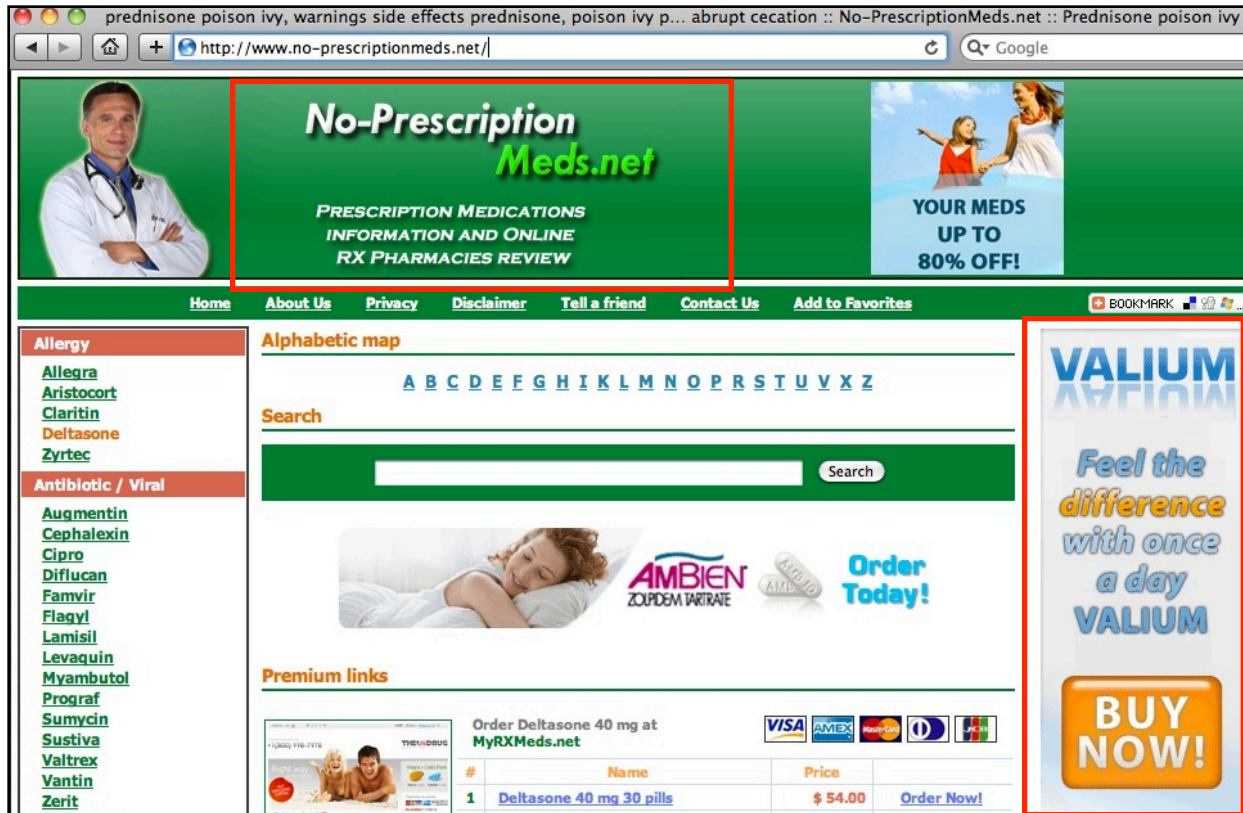
Approximately one year earlier, LegitScript had provided information to eNom about four websites selling prescription drugs without requiring a prescription. All four of these are still registered with eNom, and three of the four are still online. (It is unclear why there is no content at the fourth.)

- [Ordertopmeds.net](http://Ordertopmeds.net)
- [No-prescriptionmeds.net](http://No-prescriptionmeds.net)
- [Buyrxtabs.com](http://Buyrxtabs.com)
- [1001medicines.com](http://1001medicines.com)

As we explained in the 2008 letter to eNom, these websites' illegal nature was easy to verify:

The(se) websites offer to sell controlled substances without a prescription from overseas. This is a violation of US federal law and every state law in two respects: first, controlled substances may not be possessed or dispensed in the absence of a valid prescription; and second, controlled substances may not be imported directly to the customer from outside of the United States.

Here, we want to emphasize that the websites' illegal activity is clear on its face: there is no possible interpretation of these websites' content that indicates that they are operating lawfully. This is different from — for example — a website engaged in "spam" email or malware, where a Registrar may require proof of the spam or some quantum of public complaints before acting. The website's illegal activity is open, notorious and unambiguous.



As of the writing of this report, the websites are still online. As shown below, websites such as no-prescriptionmeds.net overtly continue to sell prescription drugs without requiring a prescription, including links to websites selling controlled substances such as Valium or OxyCodone.

In short, we provided eNom with the same type of information — indeed, in most cases, exactly identical information — of criminal activity that we provided to GoDaddy, Spirit Domains, and the other Registrars who quickly or eventually suspended the domain names. The criminal activity was indisputably clear, including screenshots of websites selling drugs without requiring a prescription, and letters from government agencies confirming that pharmacy licenses were forgeries.

### **eNom's response: "We're just the Registrar."**

Unlike most Registrars to whom we provided information, eNom elected to allow the domain names to continue using the company's registration service to remain online. Later in this report, we analyze the company's responses more closely, including eNom's, and explain why domain name registration services are an integral part of these illegal websites' strategy to stay in business.

At the outset, we note that the common thread through the eNom’s various responses to us was that it is “only the Registrar”, or that the company lacked sufficient information to conclude whether the websites shown above were acting illegally. On some occasions, eNom stated that we should contact the ISP (host) where the website content is hosted, but steadily declined to take any action to prevent these websites from using the company’s domain name registration services. eNom also indicated that it would not take any action without a court order, even after receiving screenshots showing that the websites were selling drugs without a prescription, and letters from government regulators confirming that the pharmacy licenses were forgeries. Yet, if these excuses are valid, why did most other Registrars suspend identical websites based on the same information, but eNom did not? We dissect these responses from eNom later in our report.<sup>13</sup>

Below are ten sample websites — out of over 4,000 — that utilize eNom’s domain name registration services and that either have a fake pharmacy license or are engaged in other drug-related criminal activity that the authors notified eNom about, but that as of this writing, months after our notifications are still online and utilizing the company’s domain name registration services.

eNom-registered domain	
buyviagrasuperactive.com	no-prescriptionmeds.net
canadianfamilypharmacy.org	anxiety24hs.com
canadianhealthcaremail.net	noprescription.biz
canadianhealthcareshop.org	sc-rc.com
cheap-pharmacy.us	buynoprescriptiondrugs.com
legalrxmedications.com	internationaldrugcompany.com
pharmacyfit.com	rimonabantplus.com
buyaccutanehere.com	easyprescription.us
buycialissuperactive.com	order-cheap-cialis.info
canadianpharmacynetwork.org	pharmasellers.com

---

<sup>13</sup> The authors note that some of the websites appear to have been disabled or suspended for other reasons, apparently including spam. Several of the websites now are redirected to a blank page by a server called blockedduetosпам.pleasecontactsupport.com, indicating that spam, but not the illegal sale of pharmaceuticals, is the reason for the suspension. Please see our discussion, later in this document, of why suspending domain names for spam is a good policy, but is not a sufficient approach to the problem of rogue Internet pharmacies or other similar criminal activity.

## CentroHost

CentroHost is an ICANN-accredited Registrar located in Russia. Importantly for the purposes of our analysis, CentroHost is under the same corporate umbrella as Galant-Park-Telecom (GPT), an Internet Service Provider (ISP, or “host”). The reason that this is important is, in many cases, the Registrar and hosting company for a given website are two separate companies, and often leverage this point to shift the blame when asked to shut down an illicit website. With CentroHost, the parent company is not just the Domain Name Registrar for some of the websites displaying a fake pharmacy, but also hosts the illicit content in its capacity as Internet Service Provider.



Of the 177 websites that we notified CentroHost about, forty-four (44) were still online at the time of this writing. Although this may initially appear to indicate partial compliance, it appears that at least some of these simply expired (e.g, the registration period ended naturally and the website registrant did not renew the domain name), and in its email to us, the company explicitly declined to take action other than disallowing the customer from registering additional domains, as described below.

### CentroHost Terms and Conditions

CentroHost’s Terms and Conditions are written in Russian, but a translation convincingly details the company’s requirement that domain names only be registered from lawful purposes. The “Dispute Resolution Rules” accessible at [centrohost.ru](http://centrohost.ru) provide what appears to be a fairly direct translation of the Uniform Dispute Resolution Policy language. Translated from the Russian:

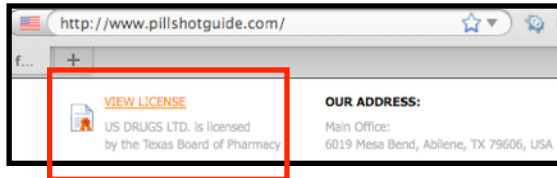
- 2. Your approval.** In applying for the service domain behalf of, or support service domain registration or renewal of a domain name, you hereby warrant to us that
- (C) you are not registering the domain name for an unlawful purpose;**
  - (D) you will not knowingly use the domain name in violation of any the applicable laws or regulations.**

Similarly, the domain name registration agreement for .com domain names (again, translated from the Russian) states that the registrant “confirms the fact that (customer) has read and agrees to...the Uniform Dispute Resolution.”

### Notification to CentroHost

We notified the company about 177 websites displaying a fake pharmacy license, and attached the letters from the Boards of Pharmacy confirming that the licenses are forgeries, explaining — as we did for other Registrars — that the pharmacy licenses are fake; the website are selling prescription drugs without a prescription; the websites illegally import prescription drugs; and are selling fake or banned products like “female Viagra.”

Among the websites we notified CentroHost about were [pillshotguide.com](http://pillshotguide.com), which proclaims itself as “U.S. Drugs” and urges Internet users to “BUY QUALITY DRUGS from the US based pharmacy.” As with several of the websites we notified eNom about, the website states that it is licensed in the State of Texas, and even displays a pharmacy license purportedly from Texas (or Ontario, etc.).



Our notification to CentroHost, as with all of the Registrars, included a letter from the Texas State Board of Pharmacy on its official letterhead stating:

On November 18, 2009, you provided information to the Texas State Board of Pharmacy (TSBP) indicating that numerous websites selling pharmaceutical products are falsely claiming to be licensed in the State of Texas. Specifically, you provided a certificate that is displayed or linked on Internet websites to a "Drug Reselling License" (#03161490), provided to US Drugs Ltd., 6019 Mesa Bend, Abilene, TX 79606 (see enclosure).

The license above-referenced license (sic) was not issued by TSBP. In addition, US Drugs Ltd. is not licensed by TSBP.

We heard back from a CentroHost employee who asked us if we planned to file a complaint with the National Arbitration Forum — a method of pursuing domain name-related trademark violations. We explained that the National Arbitration Forum is relevant to trademark disputes, but not to criminal activity, and our complaints related to illegal activity, not intellectual property violations, so the NAF was not the right venue.

Moreover, as we pointed out, this Internet drug ring was operating approximately 8,500 websites; even if the National Arbitration Forum were the right venue, the costs for filing complaints regarding such websites would apparently have cost us over \$1,000,000, simply to complain about easily verifiable illegal activity.

CentroHost replied, stating that the UDRP rules are "applicable only if the 3rd party starts official NAF process" (sic). We explained to CentroHost that this is simply not true. No other Domain Name Registrar suggested we contact the NAF.

CentroHost next indicated that they would not consider the letters we sent from the Boards of Pharmacy attesting that the pharmacy licenses were forgeries, because "Russian law does not see scanned documents as valid documents", insisting that only signed originals could be considered.

We then offered to procure signed originals and send them to CentroHost. CentroHost did not directly respond to our offer of signed originals, but then indicated that even if we sent them signed originals, they could only act if they had a court order issued by a Russian court, because:

If we suspend these domains the (customer) can and will sue us ... and will eventually win the case.

We explained to CentroHost that this is incorrect, pointing out that:

You do not need the decision of a local court. Other Registrars, such as GoDaddy, Directi, SpiritDomain...and numerous others have suspended identical domains based upon the information we provided. Indeed, ICANN assumes, by accrediting a company as a Registrar, that they are competent to enforce their own Terms and Conditions and the UDRP. You do have the contractual authority, once you are given notice that a domain name violates those terms, to suspend the domain name.

Although the authors note the company's stated promise not to allow the customer to register additional domain names, the websites listed below are, as of the writing of this report, still online, and still displaying fake pharmacy licenses — and are registered with CentroHost.

<b>Sample Websites Still Online and Registered with CentroHost</b>	
aroundtheworldmeds.com	bestrxmedspills.com
canadianqualitymeds.com	pilltabletspharmacydirect.com
buypillsdirect.com	pilltabletspharmacyonline.com
canadarxmeds.com	rxhealthpillsdiscounts.com
bestcatmeds.com	quadrhealth.com

## Realttime Register (Netherlands)



Realttime Register is located in the Netherlands. According to LegitScript's data, it is the sponsoring Registrar for over 325 illegal Internet pharmacies.

At the outset, it is important to note that the company did suspend the websites we notified them about displaying a forged pharmacy license. However, the point of this report is not that a letter from a government agency should be required (indeed, most Internet drug rings' websites do not display any pharmacy license at all, forged or otherwise), but rather that if a Registrar becomes aware that its services are being used in furtherance of criminal activity, that it is bound to act.

Of the thousands of illegal Internet pharmacies in existence, one of the most prominent is called XLPharmacy.com: unlicensed in the jurisdictions it ships to, it does not require a prescription and sells unapproved substances as prescription drugs. As shown below, we gave Realttime Register clear information that the company is wholly illegal — but Realttime Register chose to allow the company to continue to use its services in the furtherance of criminal activity.

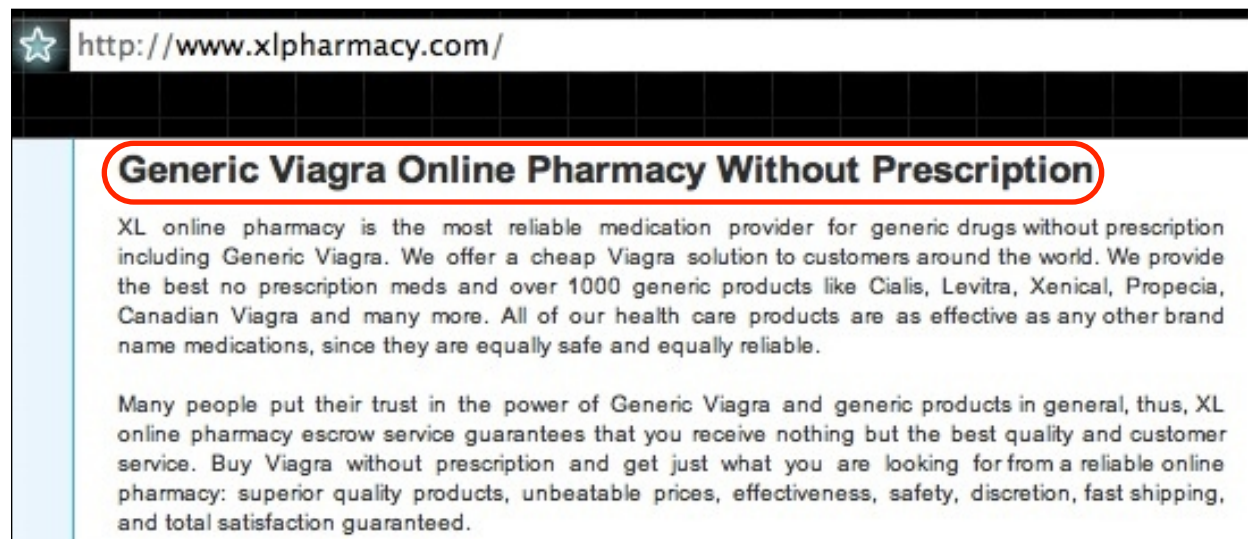
### Realttime Register's Terms and Conditions

As are all ICANN-accredited Registrars, Realttime Register is bound by the Uniform Dispute Resolution Policy, which is quoted earlier in this document as prohibiting the registration of a domain name for an unlawful purpose.

### Notification to Realttime Register

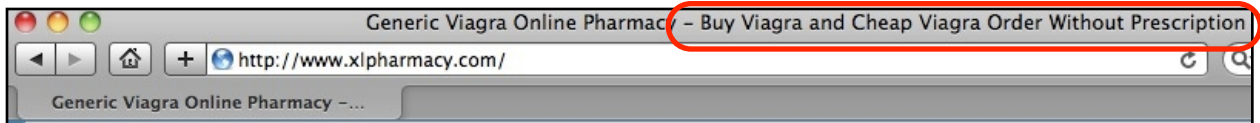
The authors provided clear evidence to Realttime Register that XLPharmacy.com is operating illegally. Noting that this law is the same in most countries worldwide, we pointed to the US law<sup>14</sup> prohibiting the sale of a prescription drug without a prescription. This is a criminal offense.

Our notification included the following screenshots showing that XLPharmacy.com sells drugs without requiring a prescription.




<sup>14</sup> 21 USC 353(b)(1) states that "a drug intended for use by man... shall be dispensed only (i) upon a written prescription of a practitioner licensed by law to administer such drug."





http://www.xlpharmacy.com/tamiflu/

## Tamiflu



Tamiflu (Oseltamivir Phosphate) is an antiviral oral drug used for the treatment of influenza A, B and swine flu in patients who have shown symptoms during 2 days or less.

Tamiflu works by preventing the growth and spread of the flu virus in your body.

Oseltamivir Phosphate shortens the period of time you have flu symptoms such as nasal congestion, cough, headache, sore throat, fever, muscle aches, chills and tiredness.

You should continue taking this medication even if you begin to feel better.

Do not stop taking the treatment without talking first to your doctor.

Tell a friend


Brand Name: **Tamiflu**  
 Manufacturer: [N/d](#)  
 Exp Date: **Apr-2012**

Availability: Out Stock  
 Average Delivery Time: **10 days**  
 Prior Prescription Required: **No**

Bookmark us

http://www.xlpharmacy.com/generic-clialis/

## Tadalafil



Tadalafil is an oral medication classified as a PDE5 inhibitor that is used to treat a male sexual problem called erectile dysfunction (a.k.a. impotence). Tadalafil works by relaxing the muscles and increasing the blood flow that goes particularly to the genital area and the penis. This chemical blocks the PDE5 (phosphodiesterase type 5) enzyme in the body, which in combination with sexual stimulation helps to achieve and maintain an erection.

Tell a friend


Brand Name: **Tadalafil**  
 Manufacturer: [Cipla](#)  
 Exp Date: **Apr-2012**

Availability: In Stock  
 Average Delivery Time: **10 Days**  
 Prior Prescription Required: **No**

Quantity	Strength	New Customer		Returning Customer	
		Price	Unit Price	Price	Unit Price
40 Pill	20 mg	\$89.00	\$2.23	\$80.10	\$2.00

http://www.xlpharmacy.com/generic-xenical/

## Buy Generic Xenical Online - Orlistat



Generic Xenical marketed under the trade name Xenical by Roche, also known as tetrahydrolipstatin is a drug designed to treat obesity.

Generic Xenical primary function is preventing the absorption of fats from the human diet, thereby reducing caloric intake.

Generic Xenical intended for use in conjunction with a physician-supervised reduced-calorie diet.

Tell a friend

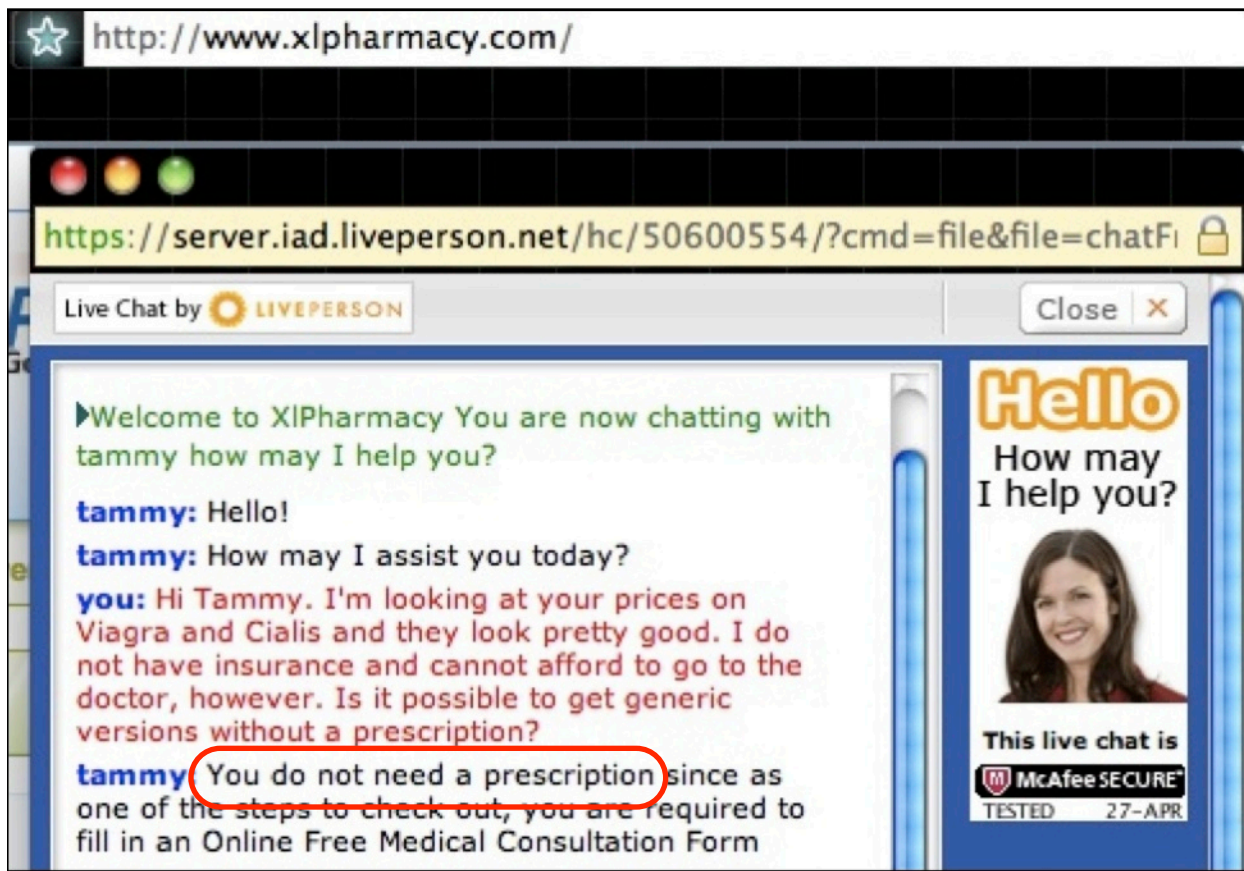
Brand Name: **Xenical**  
 Manufacturer: [Sanofi](#)  
 Exp Date: **Apr-2012**

Availability: In Stock  
 Average Delivery Time: **10 Days**  
 Prior Prescription Required: **No**

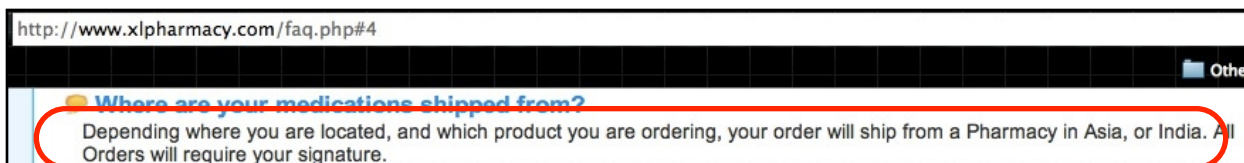
Quantity	Strength	New Customer		Returning Customer	
		Price	Unit Price	Price	Unit Price
21 Caps	120 mg	\$40.00	\$1.90	\$36.00	\$1.71

As we explained to Realtime Register, although the website states that an online doctor will review the form, there is not likely a doctor involved, since orders are immediately approved without question. Even if there were a doctor involved, this would be illegal: simply filling out an online form is not a legal basis for writing a prescription, particularly when the “doctor” is in an undisclosed country, cannot physically examine the patient, is never identified, and is not licensed in the patient’s own country.

To dispel any doubt, we engaged in a chat with the website. It clearly told us that we would not need to do anything except fill out a form. Please see the chat transcript on the next page.



Moreover, we explained that the website is overtly shipping prescription drugs illegally into the United States, Canada and other places, pointing to the law<sup>15</sup> that this violates, and then providing the following images from XLPharmacy.com. The authors also explained to Realtime Register that the company is breaking the law because it is not licensed in the locations (e.g., United States, Canada, etc.) that it ships prescription drugs to, and sells products that are not approved, including substances not approved for sale as medicines.



### Realtime Register's Response

In response to the information above, the company refused to take any action, despite being provided clear evidence that the website was operating illegally. The company's reply stated:

As the Registrar Realtime Register has no interference with the content of website (sic). We refer you to the hosting company of the site...(w)e are not

<sup>15</sup> 21 USC §331 Prohibited acts

The following acts and the causing thereof are hereby prohibited...  
The importation of a prescription drug in violation of section 804...(etc.)

qualified to establish the legality of offerings on websites, or judge the jurisdiction of foreign entities.

In response to the information we provided to Realtime Register, the company refused to take any action, despite being given clear evidence that the website continues to operate illegally, and could not continue doing so without using Realtime Register's domain name registration services. Yet, as we explain later in this report, it is precisely because Realtime Register is a Registrar — not in spite of it — that they are supposed to act to prevent the criminal misuse of their services.

## UK2Group (resell.biz)

At the outset, it is important to mention that of the 103 websites we notified UK2Group/resell.biz about four months ago, only 22 currently remain online. However, UK2Group/resell.biz refused to suspend the domain names we notified them about, even after being provided letters from the state boards of pharmacy establishing that the pharmacy licenses were fake. The reason that some of the websites are offline is unclear to the authors, but since 22 remain online, and all of the websites were largely identical, we assume that the company's position regarding its obligation to suspend illegal websites was unchanged. In total, the company's domain name registration services are still being used by over 200 websites that are part of an Internet drug ring.



Next, it is important to untangle the question of who, and where, UK2Group is. Like eNom, GoDaddy and others, UK2Group is accredited by ICANN as a Domain Name Registrar. According to ICANN's official list of Registrars, the company is located or headquartered in Gibraltar. The company's website, uk2group.com, indicates that the company has offices in London and Utah.

However, the company's registration services are handled by resell.biz, which appears to be either a subsidiary or related in some other close way to UK2Group. Indeed, when a customer seeks to register a website with UK2Group, they are directed to resell.biz. Additionally, our complaints to UK2Group were sent to, and were handled by, resell.biz. For all practical purposes, it appears that resell.biz acts as the Registrar for UK2Group.

Resell.biz, in turn, indicates that it is located in Providence, Utah, and is either located at the same address, or is the same, as WestHost, Inc., but the details remain potentially elusive.<sup>16</sup> Accordingly, it would appear that UK2Group is conducting its Registrar business from within the US, rather than from Gibraltar. Accordingly, we look to UK2Group and resell.biz as a common entity for the purposes of reviewing UK2Group's response to our notifications.

### **UK2Group/resell.biz Terms and Conditions**

If a domain name is used unlawfully, resell.biz is able to suspend domain names that violate the provisions above, including by engaging in unlawful activity. Specifically, the company's Terms and Conditions include this provision:

`SERVICE(S) PROVIDED AT WILL AND TERMINATION OF SERVICE(S): We and your Primary Service Provider may reject your domain name registration application or elect to discontinue providing Service(s) to you for any reason within 30 days of a Service initiation or a Service renewal. Outside of this period, we and your Primary Service Provider may terminate or suspend the Service(s) at any time`

---

<sup>16</sup> It is worth recounting part of our attempt to determine exactly who resell.biz is. We first reviewed the domain name registration for resell.biz. Oddly, it does not even use UK2Group as a Registrar, but instead uses eNom. The registration information as of late 2009 led to "Ditlev Bredhal" at an address in "London, Germany." One of a Registrar's most important duties is to ensure their own customers' registration information is accurate, so we were surprised to find that resell.biz's own registration appeared to be inaccurate (assuming that there is no city called "London" in the country of Germany). We consequently filed a "Whois complaint" with ICANN regarding the domain name resell.biz, which requires that the Registrar confirm the accuracy of the domain name registration information. About 30 days after we filed our complaint, rather than correct its domain name registration information, resell.biz signed up for eNom's anonymous domain name registration service, and its own domain name registration information is now hidden from the public.

for cause, which, without limitation, includes...**serious allegations of illegal conduct...**

7.1 We reserve the right to immediately terminate this TOS, and suspend or cancel your Services, and, if necessary, your domain name: (i) for a violation of any provision of this TOS or any other Agreement, including third party agreements that apply to you through this TOS; and/or (ii) your failure to pay any amounts due.

Additionally, as with any ICANN-accredited Registrar, UK2Group/resell.biz incorporates the Uniform Dispute Resolution Policy, which prohibits unlawful activity, into its own Terms and Conditions by reference, requiring that its customers:

2.15 ...agree to be bound by the ICANN domain name dispute policy (UDRP), which may be found here: <http://www.icann.org/dndr/udrp/policy.htm>.

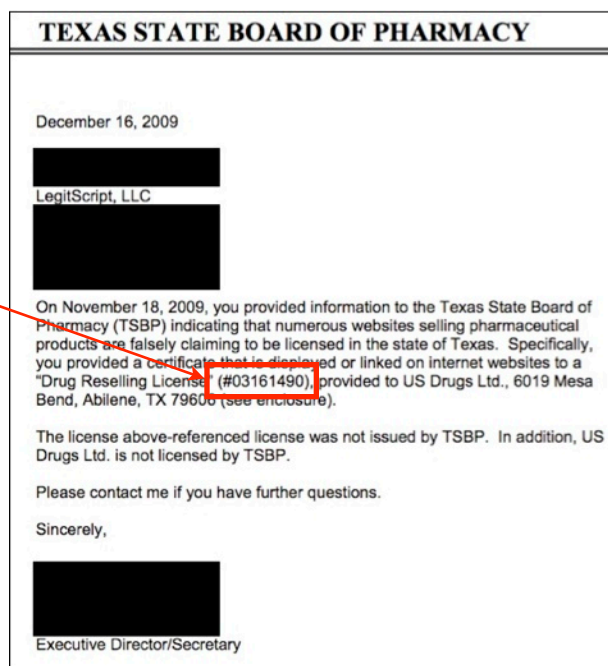
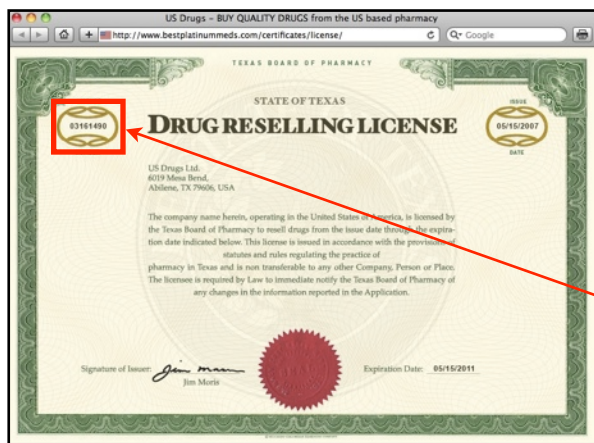
UK2Group's/resell.biz's Terms and Conditions are clear: the company can suspend a domain name if it is used in furtherance of criminal activity.

### **Notification to UK2Group/resell.biz**

As with eNom, CentroHost, and Realtime Register, the authors provided written notification, along with screenshots, to UK2Group establishing the unlawful nature of the websites in question, such as [bestpricedmeds.com](http://bestpricedmeds.com) (still online and registered with UK2Group at the time of this writing), including selling drugs without requiring a prescription; importing prescription drugs in violation of federal drug safety laws; selling fake or banned pharmaceutical products; and displaying forged pharmacy licenses.

The authors expected that a letter from the Texas State Board of Pharmacy, the government agency responsible for licensing pharmacies in Texas, attesting to the fraudulent nature of the pharmacy licenses on websites such as [bestplatinummeds.com](http://bestplatinummeds.com) would be compelling enough evidence to convince the company that the websites violate its Terms and Conditions. It was not.





### Resell.biz Response

Like eNom, Realtime Register and CentroHost, UK2Group/resell.biz told us that it would not prevent the use of its registration services by the websites that we notified them about. However, the company's response is important to dissect, and we quote most of our exchange below.

First, in response to the letters from the State Boards of Pharmacy establishing that the pharmacy licenses were forgeries, the company initially said it would "take care of the suspensions," a positive sign. But the company then said that we should contact an "approved Domain Dispute Resolution Provider" to submit the complaint instead — a signal that the company misunderstood our complaint to be based on trademark infringement.

In response, we explained to resell.biz:

Actually, this isn't a trademark or service mark complaint. LegitScript doesn't have any rights in the domain names. Therefore, there isn't any sort of a UDRP process set up for that. There are several ways to violate the UDRP and trademark is one of them, but the process itself isn't set up to deal with complaints of the type we've filed (with you), which are based on fraud and criminal activity. Several other Registrars have already suspended identical websites/domains based upon the information we've provided, so we're quite confident that filing UDRP complaints isn't required.

In response, UK2Group replied that they had contacted the reseller — a UK2Group domain name sales agent apparently operating out of Russia, where the EvaPharmacy Internet drug ring operates out of — and provided us the following response (the reseller's response is in italics):

An e-mail was sent to the owner of the domains, this is their response (*sic*). If you would like to contact them directly let me know or if you want them to contact you.

*We are based in Russian Federation domain reseller and the most part of our customers is based in Russia or CIS too. Mostly we are dealing with Search Engine Optimisers as a customers and attached domains belong to them. All the websites and products on these websites are targeted to Russian customers, so I'm not sure that US company or US agencies are responsible for control on selling in the other country products. According to Russian laws these products, websites and the way of*

*selling them is not offensive or have any criminal nature, so I'm not sure that we have any legitimate right to suspend them.*

In other words, resell.biz's reseller, who was operating out of Russia, and — like UK2Group — receiving revenue from the sale of domain names used in the furtherance of criminal activity — made the fantastical claim that the websites were only targeting Russia, not the US. We explained to resell.biz that this was provably a lie. Although lengthy, we think it appropriate to quote our entire response to resell.biz:

Whew. That's a pretty blatant lie on their part. This is really easy to see through — let's walk through the steps on the false claim that they are only targeting Russia.

1. The websites call themselves "Canadian Health&Care Mall" or "US Drugs", etc. See, for example, [greatdrugspharmacy.com](http://greatdrugspharmacy.com). They are presenting themselves as a Canadian pharmacy. Obviously, that's to target US and Canadian customers including others around the world.
2. They post a pharmacy license in Canada or US jurisdictions claiming to be licensed there. The license is fake, but quite obviously they are targeting jurisdictions outside of Russia. Of course the government agencies who wrote those letters have a stake in this. Have you seen the forged pharmacy licenses displayed on the websites?
3. Try a test order, for example, again at [greatdrugspharmacy.com](http://greatdrugspharmacy.com) — you don't actually have to make a purchase, just follow through to where you can put in your shipping information. It's about 3 or 4 steps — when you get to the order page the DEFAULT shipping option is to the United States (perhaps that's based upon our IP address; if you are outside of the US, you can easily choose the US as your shipping location).

We aren't going to contact the domain owners: This is Russian organized crime — it's a total of over 8,700 domains at about 20 different Registrars and it's a criminal network. Drug dealers don't just stop what they are doing because somebody asks them nicely. What's more, if this is one of your resellers, you need to investigate them, because their response would indicate that they are knowingly facilitating and covering up illegal activity.

We do expect that you will suspend these domains based on their clear illegal nature now that you've been put on notice. As far as whether your reseller has the "right" to suspend them, keep in mind that you are the ICANN accredited Registrar — not the reseller — and you have those commensurate obligations as an ICANN Registrar.

Please look at the websites we notified you about and the evidence we provided you. This isn't a close call.

In response to this email from the authors, and despite having provided the company evidence that these websites were engaged in criminal activity, UK2Group responded as follows:

Resell.biz...cannot lawfully 'play judge' outside of our terms and conditions and decide what is and what isn't appropriate content...(a)s an ICANN accredited Registrar we are bound to follow the UDRP once a decision has been made by an approved Domain Dispute Resolution Provider. You can find a list of approved providers here: <http://www.icann.org/en/dndr/udrp/approved-providers.htm> - citing section 2 of the UDRP in your abuse report is misleading.

"LegitScript is writing to provide you evidence about several domain names that violate your Terms and Conditions" - could you provide evidence demonstrating how these domain names have violated our terms and conditions.

Incredibly, UK2Group seemed to be saying that they couldn't see how illegal activity, which is prohibited in their own Terms and Conditions and in the UDRP, is a violation of either the company's Terms and Conditions or the UDRP. In response to resell.biz's statement that it was misleading for the authors to cite section 2 of UDRP in our abuse report, we pointed yet again to the language in the UDRP prohibiting the use of the domain name in violation of any applicable laws or regulations, as well as the company's own Terms and Conditions, quoted above.

We asked resell.biz to tell us why they could not "lawfully play judge outside (its) Terms and Conditions" if a website is clearly fraudulent and criminal. After all, the notification about criminal activity isn't outside of the company's Terms and Conditions; it's well inside of it, as we showed above. (And, isn't "playing judge" precisely what a company is *supposed* to do when a violation of its Terms and Conditions is reported?) We replied:

Please point (us) to the provision of law that prevents you from suspending domains based on serious allegations of illegal conduct — if that's illegal, then the UDRP and your Terms and Conditions need to be rewritten. Also, several other Registrars have already suspended identical domains based on the same evidence. What's more, your Terms and Conditions clearly give you the contractual authority to do so. Again, please point me to the provision of law that makes it unlawful for you to suspend these domains when you receive evidence of illegal conduct.

The authors received no response to these questions.

As of the writing of this report, UK2Group remains the sponsoring Registrar for over 200 rogue Internet pharmacies that can easily be verified as operating not in compliance with US laws (or, for that matter, the laws of other countries). Below are a few of the sample domains we notified the company about remain online and registered with UK2Group/resell.biz.

Sample Websites Still Online and Registered to UK2Group/resell.biz	
holistichealthandwellbeing.com	rxpillstabletsbargain.com
bestplatinummeds.com	supertabletpharmacyrxsite.com
greattabletspharmacyrxworld.com	wellbeingmedicationsstore.com
rxmedspillsguide.com	wellbeingprescriptionshop.com
drugtreatmentpills.com	greatdrugspharmacy.com



## Moniker (Oversee.net)

Moniker is an ICANN-accredited Registrar that provides a Florida address. The company also uses an Oregon address, while its parent company, oversee.net, appears to be in California.



From the authors' perspective, Moniker presented a somewhat different situation: we notified the company about 164 rogue Internet pharmacy websites, sending the company a 41 page letter, plus the letters from the State Boards of Pharmacy regarding those that were displaying a fake pharmacy license. Of the websites we notified the company about, 67 are still online. All but one of the websites displaying fake pharmacy licenses appear to have been shut down (we assume that the single website still online was an inadvertent omission).

For Moniker then, we express our appreciation to the company regarding the websites that were suspended based on our notification. However, the authors are concerned by the fact that the remainder of the websites, some of which are clearly offering prescription drugs and controlled substances such as OxyContin and Vicodin without a prescription, are still online and utilizing Moniker's domain name registration service. The illegality of these websites is obvious; Moniker should promptly suspend and lock the domain names through the domain names' expiration.

### **Moniker's Terms and Conditions**

Like all ICANN-accredited Registrars, Moniker's Terms and Conditions give the company the right to refuse its domain name registration services should the website be engaged in unlawful conduct:

#### **10. PROHIBITED CONDUCT**

As a condition of your use of our services, you agree not to use them for any purpose that is unlawful...and you agree to comply with any applicable local, state, federal and international laws, government rules or requirements.

...you agree that the following is a non-exclusive list of actions that are not permitted when using the services:

- promoting or providing instructional information about illegal activities...

We reserve the right to cancel or terminate your use of the services if you engage in any of the activities described above...

### **Moniker's Response**

The authors never received any response from Moniker, after providing written notification with screenshots via certified US mail. However, as noted, all but one of the websites that were displaying fake pharmacy licenses were suspended. So were several others that we notified the company about.

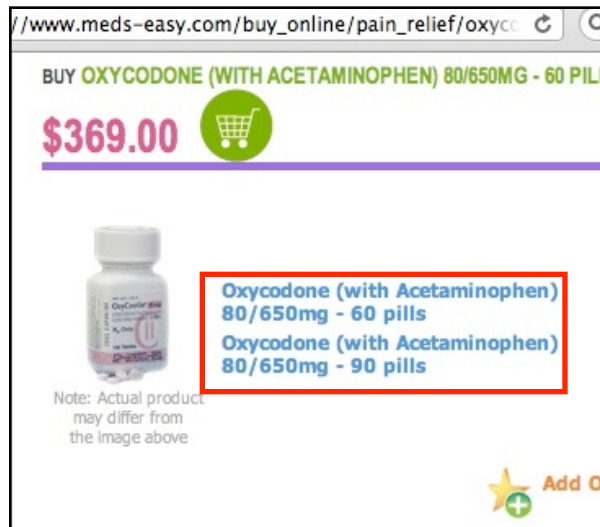
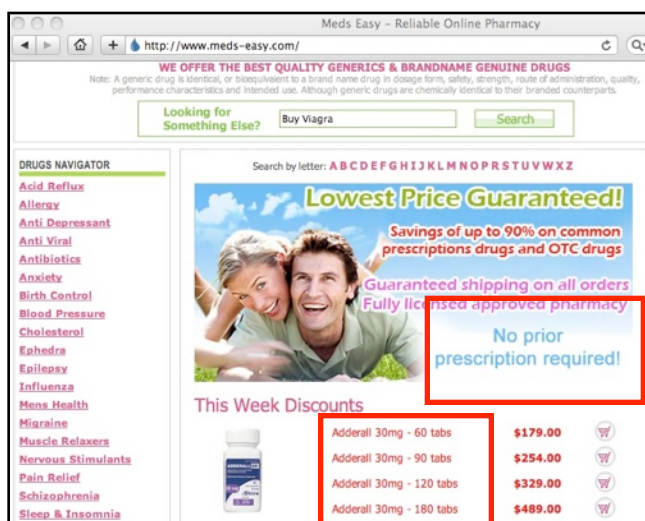
However, many of the most obviously illegal websites were left online. Our documentation to the company explained — and we presume that the company is aware — that the sale of a prescription drug without a prescription is illegal. This is especially true for controlled substances like Vicodin or OxyContin.

Below are three examples of websites that we notified the company about — in one case, for the second time — but that remain online and using Moniker's domain name registration services.

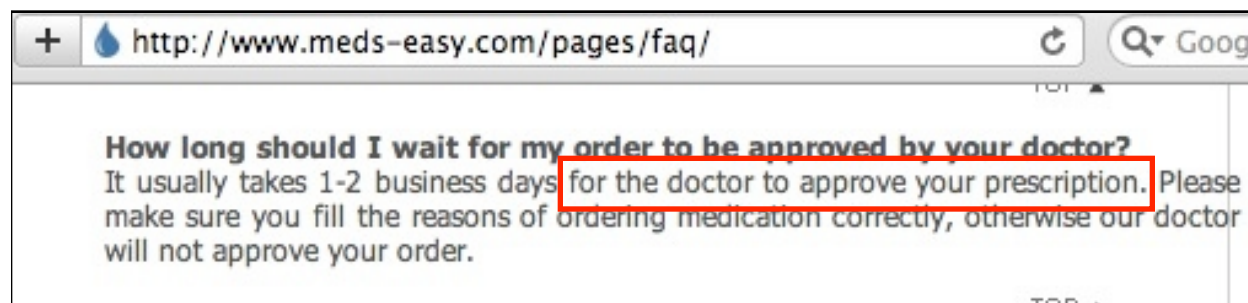
### Example 1: meds-easy.com

In 2008, LegitScript notified Directi, which was then the Registrar for [meds-easy.com](http://meds-easy.com), that the website was selling prescription drugs without a prescription. Directi promptly suspended the domain name, which remained inactive for some time. Once the suspension was lifted, the website was re-registered with Moniker. We notified Moniker about the website. Moniker did not suspend the domain name.

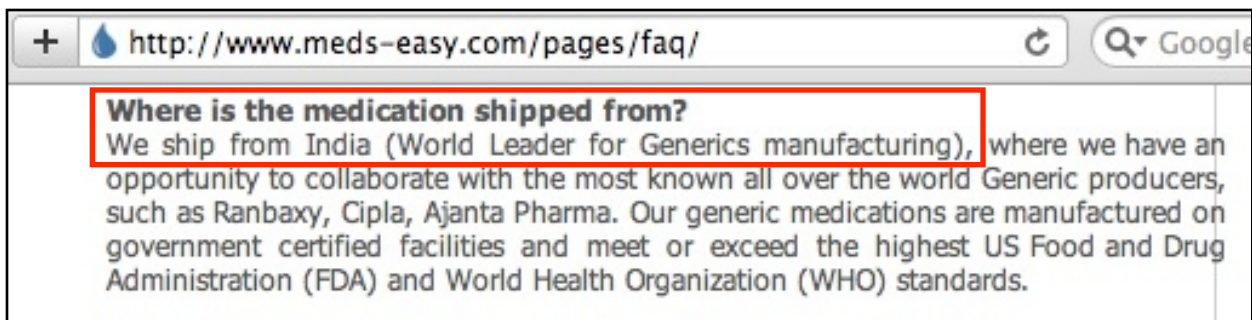
Moniker should easily be able to verify the illegal nature of this website. For example, the website clearly states that it is selling Adderall, which is a controlled substance, without a prior prescription — a per se violation of the federal Controlled Substances Act. Indeed, the website is selling OxyContin. The authors expect that Moniker's attorneys can confirm, if necessary, that OxyContin cannot be legally sold without a valid prescription.



Second, the website's own FAQs state that that an online doctor will review the order. The authors are comfortable stating that there is no doctor involved at all, having conducted prior test buys from this website (the drugs arrived from Pakistan). Even if there were, this is — as explained earlier in this document — a direct violation of the law and, because no in-person examination is required, is akin to simply selling drugs without a prescription.

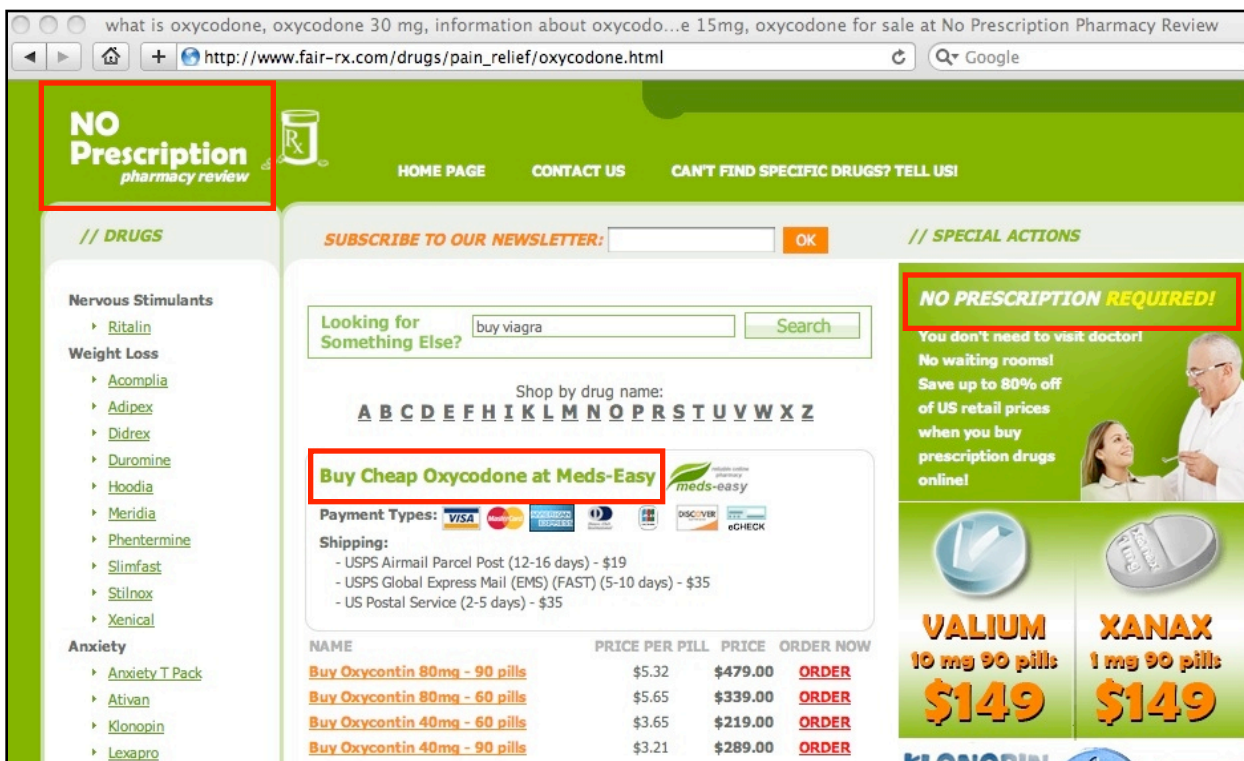


A third reason, of course, is that the website explicitly states that it is importing these drugs from India. This is a legal violation, both of the federal Food, Drug and Cosmetic Act, and because controlled substance are involved, the Controlled Substances Import and Export Act (CSIEA).



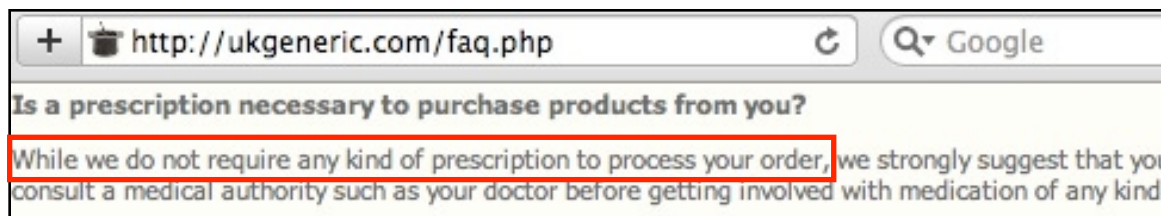
**Example 2: Fair-Rx.com**

To provide yet another example of a website that is still online with Moniker but that can easily be verified as unlawful, consider fair-rx.com. It sells OxyContin (as an affiliate to the first website, meds-easy.com), and states in several places: “No Prescription Pharmacy Review” and “No Prescription Required.” Indeed, it has “no prescription required” all over the website. Again, the authors suggest that it is fairly easy to quickly determine that this website is operating unlawfully.



**Example 3: ukgeneric.com**

Similarly, the website ukgeneric.com, registered with Moniker despite our notification, offers prescription drugs without a prescription.



Below are twelve sample websites that are still online and registered with Moniker, out of over 100. We notified the company about these websites, but they are still online and utilizing Moniker's registration services.

<b>Sample Websites Still Online and Registered with Moniker</b>		
33drugs.us	Legalrxdrugs.com	unicaid.com
myphentermine.net	meds-easy.com	qh4.net
buy-viagra-danmark.net	meds-easy.net	askcure.com
genericdrugsexpress.com	Meds-Order.com	bestedpills.com

## chapter 5 — ten common Registrar excuses dissected

As shown above, most Domain Name Registrars — Advantage-Interactive, Joker, GoDaddy, Directi and others — suspended the illegal Internet drug ring domain names we notified them about. But a few did not. Over the course of our communications with those Registrars, we heard the same responses as to why they could not, or would not, block the use of its domain name registration service by these websites.

The intent of this section is to examine the various responses that Registrars gave for declining to allow their services to be used in furtherance of the criminal activity we notified them about. We think that whether under the UDRP, the law, or simply as an obligation to do what is right, a Registrar's responsibility is clear: when put on notice about an illegal website using the company's domain name registration service, the Registrar must conduct a reasonable inquiry and, if verified, suspend the domain name.

It is also provably untrue that a Domain Name Registrar cannot do anything about the use of its services by websites engaged in criminal or fraudulent activity without a court order. The authors encourage members of the public, or members of the press, to utilize this section in any future conversations with Registrars who make the claims below — especially the claim that the company is “only the Registrar” and is not obliged to act.

Below, in narrative format, is an overview of the common excuses we heard from eNom, UK2Group, Realtime Register, CentroHost, and — even though they eventually complied with our request — Network Solutions, as to why they could not or would not suspend domain names for websites engaged in criminal activity.

### 1. “We're only the Registrar.”

— *eNom, uk2group, Realtime Register, network solutions, centrohost*

or, “We have no control over the website's content.”

— *eNom, uk2group, Realtime Register, network solutions, centrohost*

or, “You should submit a complaint to the internet service provider or website owner instead.”

— *eNom, uk2group, Realtime Register, network solutions, centrohost*

This is the most common excuse we heard from Registrars who declined to suspend illicit websites' domain names. eNom, in particular, relied on this response on multiple occasions, implying a lack of ability or responsibility to take action against websites such as [candianhealthcaremall.net](http://candianhealthcaremall.net) selling drugs without a prescription and displaying a fake pharmacy license.

To respond to this, it is first important to understand the nature of this excuse. The Registrar's logic goes like this: the content of the website is what makes it illegal, not the domain name. The content exists on a server hosted by the Internet Service Provider (ISP), not on any servers owned or controlled by the Registrar. All that the domain name is doing is pointing to the illegal content; but the domain name itself is not inherently illegal. Therefore, anybody concerned with illegal activity should contact the ISP or website owner, not the Registrar.

This argument easily falls apart when examined using common sense and logic. First and foremost, the domain name is pointing to the illicit content, and that is how the content is accessed. The Registrar *does* have control over that, even if it has no control over the content itself. As explained several

times throughout this report, every Registrar includes in its Terms and Conditions a provision protecting its right to suspend services to websites engaged in unlawful activity. In fact, Registrars are under contractual obligation to prohibit unlawful website activity in order to remain accredited by ICANN. By contrast, ISPs are under no contractual obligation to any accrediting institution, as there is no ICANN for ISPs, and indeed, some Internet drug rings simply operate their own servers.

Second, in cases such as the thousands we notified Registrars about, the website registrant has chosen to point the domain name to the illegal content. While the actual content may exist on a server, the average Internet user cannot view it without first going to the corresponding domain name. It's part and parcel of the way that the website owner expects Internet users to access the illegal content, and thus is used in the furtherance of illegal activity: helping make illegal prescription drugs accessible to Internet users.

Third, the Registrar is in a position of profiting from the registration fees it receives for the domain name registration. If put on notice that the domain name is pointing to illegal content, future re-registration fees can reasonably be understood as derived from, or related to, profits from illegal prescription drug proceeds. The domain name facilitates unlawful activity by making the unlawful content more easily accessible than it would be simply via an IP address.

Fourth, as a practical matter, there really isn't any distinction from an Internet user's point of view: the domain name and the website's content are a seamless, integrated whole — and this is especially true with a domain name like [noprescription.biz](http://noprescription.biz) (announcing that a prescription is not required) or a like [canadianhealthcaremail.net](http://canadianhealthcaremail.net) (falsely suggesting that the website is a licensed pharmacy in Canada). It lacks common sense to suggest that the domain name is not inextricably connected to the illegal activity itself.

Yet the refrain “We're only the Registrar” has nearly become a mantra for some Registrars like eNom, NameCheap (a reseller or affiliate of eNom), and others. Here, an example outside of the Registrar world may be helpful: the payment service provider PayPal and its parent company eBay. Both companies are rigorous about ensuring that, as soon as they identify an illicit Internet pharmacy using its payment services (PayPal) or listing its products (eBay), they terminate the account, refusing to allow their services to be used in the furtherance of criminal activity. Neither company has ever responded that is it “only the payment service provider” or “only the auction site”. Nobody disputes the fact that neither eBay nor PayPal are responsible for the content, but the companies have recognized that once they are aware that their paid services are being used to further criminal activity, they must respond — not turn a blind eye to it.

2. “We can't do anything without a court order.”

— *eNom, uk2group, Realtime Register, centrohost, Network Solutions*

or, “We can't lawfully play judge.”

— *uk2group*

Some Registrars such as eNom suggested to us that they could not, or would not, suspend a domain name without a court order. As noted above, UK2Group said that they could not “lawfully play judge,” yet were unable to tell us exactly what law prohibits them from enforcing their own Terms and Conditions, which prohibits unlawful activity by their customers.

This reasoning also falls apart based on common sense. The first and most obvious point is that several other Registrars in the US and around the world acted promptly and without a court order, clearly proving that one isn't required.

Second, nothing in the law (in any country) and nothing in ICANN's rules or policies requires a Registrar to obtain a court order. To the contrary, the UDRP requires Registrars to prohibit unlawful activity.

Third, cyber-criminals know, and take advantage of the fact, that the Internet is inherently jurisdiction-less, and a court order is functionally impossible in some cases — especially those involving criminal activity. (Indeed, it might be said that some Registrars are also aware of this, and know full well that insisting upon a court order is a good way to not have to deal with the complaint.)

Consider a situation where the Registrar is in the Netherlands, the website registrant is in Russia, the content is hosted on a server in China, and the website sells drugs without a prescription shipped from India to the United States. A court order is nearly impossible to acquire in this case, and even if obtained, would generally be unenforceable. That is because a basic tenet of criminal law is that the “act” that leads to the arrest and prosecution must take place within the jurisdiction where the law enforcement agency and courts have jurisdiction. In the example above, each of the actors (other than the purchaser of the prescription drugs) committed the act outside of US soil. US courts will typically not have jurisdiction over an individual or company (including a Registrar) located outside of the US. Similarly, the foreign company can safely ignore a court order, which is not enforceable outside of the US.

A response to this might be: Why not get a court order from — for example — the Russian courts, since the registrant for the criminal website is in Russia? (Or China, the Netherlands, et cetera.) Here again, jurisdiction comes into play: US laws, not Russian laws, are being broken, so Russian, Chinese or Dutch courts have no jurisdiction to issue a court order unless it is their laws that are being violated. Registrars who insist upon a court order from their own country in cases like this do so knowing that that they are demanding an improbability if not impossibility.

But what about a situation where the Registrar is in the United States, such as eNom or UK2Group? Wouldn't US courts have the jurisdiction to issue a court order? Yes, but a second requirement comes into play: standing, which can be explained as “who has the right to file a law suit (or obtain a court order).” If these websites were engaged in civil law violations (e.g., trademark infringement) against a trademark owned by one of the authors, then as a private citizen or company, we would have standing — the right — to file a lawsuit and seek a court order, or utilize one of the UDRP trademark processes. However, as we explained to UK2Group, the authors do not have any legal rights in the domain names or content — rather, we're pointing out criminal activity, not a violation of our own intellectual property rights. In criminal cases, the government, not private citizens or companies, has standing in nearly all cases, and private citizens cannot simply go to a judge and get a court order. The US does not have a system of “private prosecution,” and criminal cases in the US and worldwide are filed by the government, not private citizens.

The predictable response to this might be that only the government should notify Registrars about criminal activity. But this returns to the first problem described above: if a person in Russia ships drugs to the United States, the act takes place on Russian soil. The Russian's response will be: if I had done it while standing on US soil, it would have been illegal, but I shipped it from another country, so I wasn't on US soil and thus cannot be arrested under US law, even if I violated those laws. Unlike private companies, government agencies are bound by ancient rules involving jurisdiction and venue that originate from English common law in the 1600s — well before the Internet made it a possibility to commit a crime that makes it possible for the criminal to claim that he or she did not commit the crime in any jurisdiction at all and thus can never be held to account.

Requiring a court order is not reasonable, and neither ICANN nor the UDRP require it. When a Registrar becomes aware that their services are being used in furtherance of criminal activity, that is the point at which they are bound to respond, rather than awaiting a court order that may never come, all the

while being aware of, facilitating and profiting from, the continuing criminal activity. Indeed, several Registrars appear to similarly interpret the UDRP, as they shut the websites down immediately.

3. “We are not a law enforcement agency and don’t have the expertise to determine if the website is operating legally or not.”  
— *eNom, Network Solutions*

We heard this in particular from eNom. Again, this reasoning quickly falls apart with minimal scrutiny.

First, and most obviously, many other Registrars suspended the domain names engaged in illegal activity. Those other Registrars are also not law enforcement agencies, so it is unclear why the fact that Registrars are not law enforcement agencies is a relevant point.

Second, we think that this response stretches credibility, especially for websites that overtly sell drugs like OxyContin or Cialis without a prescription, or post a forged pharmacy license. Are eNom, UK2Group and the other Registrars truly unsure whether these websites are acting unlawfully? The point of this report was to provide Registrars with evidence that any layperson could understand, including letters from regulatory agencies stating that the pharmacy licenses were fake.

Third, have the Registrars thought about simply asking? After all, eNom received a letter from the National Association of Boards of Pharmacy — the organization that represents the *government agencies* that license pharmacies and pharmacists — identifying LegitScript as an authority recognized by the NABP to help determine the legitimacy of Internet pharmacies, and explain what is legal and what is not. Even if one were to assume that eNom was genuinely unsure what the law requires in this area, the fact that it did not even make a cursory effort to ask suggests that the company simply isn’t interested in knowing.

Fourth, most of these companies have legal divisions and abuse teams. Presumably, trained attorneys at the company can verify that it is illegal to sell drugs without requiring a prescription. The laws on this are clear. At least in the US, for eNom or UK2Group to look at a website that states it will sell prescription drugs without requiring a prescription and respond that they can’t tell if it is acting unlawfully makes little sense. While the Registrar itself may not be a law enforcement agency, a Registrar who employs legal counsel presumably has ready access to its legal team to help determine legality in such cases.

4. “Even if the website is illegal, we will get sued if we suspend the domain.”  
— *centrohost*

No, they won’t, for two reasons.

First, all of the Registrars’ Terms and Conditions give the Registrar the right to suspend a website if, in the Registrars’ sole discretion, it concludes that the website is acting illegally. That’s a binding contract, and the registrant has agreed that they have no rights to sue the Registrar if the domain name is suspended.

Second, as a practical matter, a person who is illegally selling prescription drugs and posting fake pharmacy licenses isn’t going to sue a Registrar for shutting the website down. Criminals operate in the shadows: they are going to hide their identity, not announce it via a lawsuit.



5. “The Uniform Dispute Resolution Policy only pertains to trademark disputes”  
— *uk2group*

UK2Group (resell.biz) insisted to us that the UDRP only pertains to trademark disputes, and that by citing the UDRP in support of our complaint regarding illegal activity, we were being “misleading.”

There is no defense for this position. The language is in black and white:

2. Your Representations. By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that **...(c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations.**

Every Registrar is bound by this language, and its Terms and Conditions must include, at a minimum, this or similar language.

6. “You’re applying US law worldwide!”  
—*UK2Group reseller*

or, “It’s only a problem if it violates the law of our country (where the Registrar is located).”

— *centrohost*

This was part of the thrust of CentroHost’s argument, as well as the Russian UK2Group reseller re-quoted earlier in this document: that the authors are taking US law and applying it worldwide.

To understand how nonsensical the argument is, consider its reasoning, which goes like this: Even if the website is illegally targeting the US (among other countries), it is sending the drugs from (not to) India (or Pakistan, Russia, China, etc.) without a prescription, so is not violating those countries’ laws. Furthermore, there might be some country *somewhere* that doesn’t prohibit prescription drug importation or selling drugs without a prescription. Therefore, since this might be legal somewhere, as long as it isn’t illegal everywhere, it should be permitted.

The first and most obvious response to this is: the websites are targeting, and marketing to, the places where it *is* prohibited, like Japan, the UK, the US, Canada, and European countries. In these countries, incomes are higher (leading to more disposable income to acquire prescription drugs) and all have laws about the sale of prescription drugs. If the allegation is that it’s legal in, say, Russia, then there is a very simple solution: the default shipping location shouldn’t be the “United States,” and the possible shipping destinations that can be selected on the website should be restricted to locations where the company is licensed and acting in accordance with the law.

As part of this argument, the authors were frankly flabbergasted that UK2Group could, in its reply to us explaining why it “couldn’t play judge” as to the website’s illegal nature, quote its Russian reseller as stating that the websites were only targeting Russia, so wasn’t illegal. The websites, on their face, refer to themselves as Canadian or US pharmacies, are in English, and display a fake pharmacy license from the US or Canada, not from Russia.

Second, the UDRP doesn’t specify the jurisdiction where the criminal activity is to occur, and there is a reason for that: as explained above, the Internet is inherently jurisdiction-less. If all Registrars took this position, cybercrime would be something that nobody could ever do anything about, because the

Internet drug rings could make sure — as they currently often do — to ship the drugs to every country in the world except the one where the Registrar is located.

Third, along those same lines, by mandating that websites will not act “in violation of any applicable laws or regulations”, the UDRP essentially says that a website must be in compliance with the laws of any and all jurisdictions with which it does business.

## 7. “Registrars in the United States are protected by the Communications Decency Act.”<sup>17</sup>

This is generally incorrect, at least regarding the sort of cases outlined in this report, but requires some explanation.

In the United States, ISPs, Registrars, search engines and similar companies are generally protected from liability for somebody else’s conduct by a law called the Communications Decency Act. This law protects Internet Service Providers and other third-party actors from liability in a number of situations, particularly when publishing information provided or transmitted by others. A basic example of this would be a website engaged in defamatory activity and that shows up on yahoo.com as a search result, or is registered with GoDaddy, or is hosted with an ISP. The effect of the CDA is, the aggrieved party generally cannot sue Yahoo or GoDaddy or the ISP, since those parties did not “publish” the content. If those parties receive a court order, they are bound to act, but as long as they do not play an active part in creating the defamatory content, they are normally not responsible.

However, the CDA does **not** shield these third parties from criminal liability, including the knowing facilitation of a third-party’s criminal activity or knowingly profiting from that criminal activity. Indeed, 47 USC 230 (e) specifically provides, in relevant part:

### **(1) No effect on criminal law**

Nothing in this section shall be construed to impair the enforcement of section [223](#) or [231](#) of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or **any other Federal criminal statute** (*emphasis added*).

### **(3) State law**

Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

As we explained to the Registrars, the activity that we were notifying them about is criminal in nature — not civil. As a basic tenet of criminal law, Registrars cannot be held accountable for the information if they do not know about it, but once put on notice about criminal activity, a compelling argument exists that they no longer enjoy the protections of the federal Communications Decency Act, if they knowingly continue to allow their domain name registration services to be used in the furtherance of criminal activity.

---

<sup>17</sup> Although we did not hear this reasoning from any Registrar, it presumably forms the backbone of part of the US-based companies reasoning, or is at least a potential response sufficiently important that the authors believe it important to address.

8. “We sent your complaint to the website registrant, and they said they are operating legally.”  
— *uk2group*

In some cases, Registrars have indicated that they asked the customer if they were operating illegally or not, and stated that the website registrant showed them a pharmacy license, or simply said that they were not operating illegally. The Registrars then declined to suspend the website based on the customer’s representation that they were acting lawfully.

First, although the inclination to ask a registrant to provide an explanation is reasonable, Registrars should understand that if that person is involved in an Internet drug ring, they are unlikely to admit breaking the law. It is incumbent upon the Registrar to make an independent determination, not simply take a customer’s word for it that they are a legitimate, licensed entity. This is especially true when the Registrar has been provided with proof from a pharmacy licensing authority that the license is fake, or the criminal activity is obvious and can be easily verified, such as selling drugs without requiring a prescription.

Second, when Internet drug rings operate, they have to send the drugs from *somewhere*, so a licensed pharmacy is sometimes involved. That still doesn’t make it legal, or the drugs real. Indeed, what the authors have repeatedly observed is, a pharmacy in (for example) Argentina or Moldova will ship drugs without a prescription around the world to places where they are not licensed, and where it is plainly illegal to import prescription drugs. When complaints come in, the pharmacy shows an Argentinian or Moldovan license, arguing that they are therefore a legitimate actor. While such a license may make them legitimate in Argentina or Moldova, it does not authorize them to ship drugs anywhere else.

It is important to understand that a pharmacy is only regulated where it is licensed. This means its own regulatory agency can ensure only that the pharmacy sells legitimate drugs and requires a prescription for drug orders within its jurisdiction — nowhere else. This is how Internet drug rings are able to sell counterfeit or adulterated medications: the “pharmacy” is not necessarily sourcing the drugs from a regulated supplier, since by sending the drugs outside of its own jurisdiction, it is not subject to its own country’s drug safety protections. Even licensed Canadian pharmacies are under no obligation to dispense the same drugs to non-citizens that they would to Canadians, and often ship drugs to US residents from India or Turkey that could not lawfully be dispensed to Canadians.

Finally, it is important to remember that the sale of prescription drugs without a prescription, or importation of prescription drugs, is illegal, without or without a pharmacy license. The existence of a pharmacy license is not what makes an Internet pharmacy legal; it’s where the pharmacy is licensed, and whether or not they adhere to those requirements, that are the determining factors.

9. “So, you want us to police every website.”

The authors agree that this is unrealistic. It is not possible, and should not be expected, that Registrars will monitor every website that is registered with their company.

However, what we do think is required of the Registrar is to take reasonable steps to investigate once notified about a registrant’s criminal activity. If a Registrar is unaware of the illicit content of a website, it is under no obligation to act or affirmatively conduct research. However, if credible information is reported involving criminal activity, that is the point at which the Registrar cannot simply turn a blind eye to the behavior. While a Registrar does not need to take extraordinary actions (for example, conducting a test purchase of the drugs and submitting them to be tested for counterfeiting analysis), a reasonable review to see if the website is — for example — selling drugs without a prescription or illegally importing prescription drugs is an entirely appropriate expectation and response.

As explained above, merely asking a domain name registrant whether their conduct is legal or illegal is not a sufficient response. The answer will predictably be: “Yes, of course I am operating legally.”

10. “We’ll only shut illegal prescription drug websites down if they are engaged in spam and/or used incorrect registration information.”

— *Network Solutions*

Most Registrars are fairly good about suspending domain names that engage in spam. Also, one of ICANN’s core requirements regarding accredited Registrars is to require that domain name registration information — so-called “Whols” information — is accurate. In particular, if a complaint has been submitted to the Registrar regarding inaccurate Whols information, a Registrar can face penalties from ICANN if it does not require the Whols information to be corrected, and must suspend the domain if the information is not updated.

However, suspending websites for spam and inaccurate Whols registration information is a very different matter, and is not the subject of this report. We note this because some of the domains that we complained to eNom, UK2Group and other Registrars about were apparently suspended for what appears to be other reasons, such as spam or inaccurate Whols information. Indeed, Network Solutions initially told us that they could suspend a website for inaccurate Whols information, but not for evidence of criminal activity. The relevant question is not just whether the domains were suspended, but why.

There are three important points to make about this. First, much of the reason that Domain Name Registrars are fairly quick to suspend domain names engaged in spam or with inaccurate Whols information is because ICANN has insisted upon it. The approach that ICANN takes to any issue is highly relevant, and part of Registrars’ responsiveness - or lack thereof - in this area can be attributed to ICANN.

A second, related point is that neither spam nor fake Whols registrations are an end in themselves: the reason that spam is objectionable is not just because it is uninvited, but also because its content is seen as either potentially objectionable or even dangerous, as is the case with counterfeit medicines or the sale of drugs without requiring a prescription. For Registrars to take a firm stand against spam, but not the dangerous commercial activity itself that spam is used to promote, is to take a stand against the means but not the end, viewing only the process as problematic but not the undesirable and potentially dangerous or illegal result.

Third, consider Network Solutions’ (which eventually complied) initial statement that they could only suspend a domain name for incorrect Whols registration information. In addition to not being factually accurate statement, many Registrars now offer “proxy” (anonymous) domain name registration information. Criminals prefer anonymity, and by offering a proxy registration to these websites, the ability of Internet users to challenge the accuracy of the website registration is removed, because nobody can see the registration information except the Registrar.

Accordingly, while it may be true that some domains the authors submitted complaints about are now offline, and may have even been suspended by the Registrar, eNom, UK2Group, Realtime Register and CentroHost were clear with us that they would not suspend services to websites based upon evidence of a forged pharmacy license or the sale of prescription drugs without a prescription. The question presented in this report is not about spam or invalid Whols information; it is about illuminating the response that different Registrars give to a clear showing of criminal activity.

## conclusion

**Approaching adulthood, the Internet is a smashing success:** it has offered a level of intellectual, personal and commercial freedom and exchange unprecedented in human history. But it is also a success because it has structure. This structure is built on a set of commitments between ICANN and the Registrars it accredits, and is intended to ensure the growth of the Internet in a way that fosters legitimate personal and commercial activity, but prevents an out-of-control explosion of fraud and crime.

One of the basic tenets that the Internet is built upon is simple: Registrars must prohibit the use of their registration services for unlawful purposes. Clearly, with hundreds of millions of websites in existence, Registrars cannot constantly monitor every domain name registered with their company. But if put on notice about criminal or fraudulent activity, particularly with compelling and clear evidence, Registrars are supposed to act promptly to prevent the use of their registration services in furtherance of the illegal or fraudulent actions.

Why is this important? There are various types of crime, but “rogue” online pharmacies strike at particularly vulnerable populations: the sick, the addicted, and often the needy or elderly. Worldwide, billions need medications that are safe, effective and affordable; the promise of the Internet to meet this challenge is corrupted by criminals who sell fake or diluted drugs. Similarly, prescription drug addicts are a tempting target for Internet drug rings who seek to profit from others’ abuse and addiction. And the Internet user with a pressing need for an expensive medication will no longer view that “online bargain” as such a great deal when the drugs never arrive, or are found to contain no active ingredients. Given the potential profit involved, it should come as no surprise that criminals turn to Internet drug rings such as EvaPharmacy, seeking to make a buck at the expense of those who often can least afford it.

**But to do this, cyber criminals need safe havens.** Like a heroin or crack dealer looking for the right street corner, Internet drug rings need safe Registrars that can be relied upon, whether through the Registrars’ inattention, or a conscious decision to turn a blind eye to criminal activity, not to prevent the use of the company’s registration services in furtherance of illegal activity.

In this respect, it is important to clearly understand what this report is not: It is not a report about Registrars who are unaware that their paid services are being used in the furtherance of criminal activity. Rather, it is a report documenting that these Registrars were informed about the use of their registration services in furtherance of criminal activity and did nothing, or not enough, about it.

There are Registrars that, to their credit, criminals now know are not safe havens for Internet criminals: GoDaddy, Directi, SpiritDomains, Advantage Interactive, and others. The authors applaud these Registrars.

What about the other Registrars — eNom, UK2Group, Realtime Register, Moniker and CentroHost? Registrars are not law enforcement agencies, true. But being a Registrar does not mean being devoid of any responsibility at all. The Uniform Dispute Resolution Policy, which “applies to all Registrars” according to ICANN, mostly covers trademark disputes. But it also clearly prohibits the use of the domain name for unlawful purposes.

Part of the purpose of this report is to document the submission of evidence to Registrars that was so clear that a Registrar could not credibly claim an unawareness of the website’s illegal nature. Provably forged pharmacy licenses; the sale of drugs, even OxyContin and Vicodin, without a prescription; the sale of fake or banned drugs; and illegal drug importation. Any one of these would suffice to easily understand the website as operating unlawfully; in most cases above, all of the criteria were present. Indeed, most Registrars responded in a matter of days to suspending their services to these websites.

What about the claims presented by eNom or UK2Group to this, that it is “only the Registrar” and presumably cannot (or need not) do anything about the websites? Or, eNom’s insistence that it cannot (or will not) shut down the website without a court order? The most obvious evidence against these responses is that 11 other Registrars promptly suspended the illegal domains. A court order is provably unnecessary, and companies like resell.biz who said they cannot act without one cannot point to anything in ICANN requirements, or in the law, requiring them to have one. Indeed, it legitimately raises the question of why, if Registrars like Realtime Register know that their paid services are being used in the furtherance of criminal and fraudulent activity, they do nothing about it.

**The notion that a company is “only a Registrar”** also fails to understand the reality of the Internet today. Internet users access content by typing a domain name; the domain name points to the illegal content; and often, the domain name is relevant to the content (e.g., [noprescription.biz](#)). From an Internet user’s standpoint, there isn’t much (or any) practical distinction between a website, domain name, and the content: it’s a seamless whole, and if the domain name is inaccessible, for most Internet users, so is the content. What’s more, the UDRP requirements are clear: Registrars are obliged to prohibit unlawful website activity. By contrast, ISPs have no similar accreditation requirement, and in some cases, criminals simply operate their own servers. From a legal perspective, once a Registrar is put on notice regarding specific and verifiable acts about criminal activity facilitated by their services, they need to consider that if they do nothing about it, they may be viewed as knowingly tolerating it. In short, Registrars are bound to act precisely because, not in spite, of their status as Registrars.

What about an argument against censorship? Is this report actually a tale of five Registrars who heroically stood up for free speech and freedom on the Internet? No. Selling fake drugs, selling addictive medications without a prescription or any age verification, and lying about a pharmacy license are simply not in the same category of exercising one’s right to decry government authoritarianism, protest high taxes, or view constitutionally protected content that others might find offensive or obscene. After all, the actions identified in this report would be equally illegal and dangerous whether or not the Internet is involved. Put another way, one can’t magically transform acts that are criminal, dangerous and fraudulent when the Internet is not involved into a “free speech” or “censorship” issue simply by using a website to commit the crime. Whether offline or online, the sole objective of the Internet drug ring identified in this report is to make money by defrauding people. The notion that a Registrar is acting honorably by protecting the right of such websites to continue tricking people is nonsense, and conveniently ignores the fact that Registrars have a profit motive in registering as many websites as possible.

**This conclusion would not be complete without a word about ICANN**, the organization responsible for ensuring compliance with its own rules and policies. Ultimately, the entity that will have the most influence over whether Registrars adhere to ICANN’s policy requirements is ICANN itself. In this regard, ICANN’s mission is not to be some sort of champion or proponent for Domain Name Registrars, as if Registrars are collectively a republic with ICANN as its democratically elected head. Rather, ICANN’s mission is to ensure the stability and structural integrity of the Internet; part of its mission is to require adherence to a set of policies whether a Domain Name Registrar likes it or not. Put another way, ICANN needs to ensure that it does not view itself as primarily accountable to Domain Name Registrars, even though Registrars provide much of ICANN’s financial support via registration fees. Rather, ICANN should understand that its most important constituency is the world’s Internet users who want to see the Internet grow and succeed, but not spin out of control. Internet users, in turn, need to hold ICANN accountable.

But today, websites like [canadianhealthcaremall.net](#) — displaying a forged pharmacy license, selling drugs without a prescription, illegally importing drugs and selling unsafe substances — still survive. When Registrars like eNom or UK2Group ignore the clear language of their obligations and provide criminals with a safe haven, such websites thrive. We congratulate Directi, GoDaddy, and the other Registrars who, in accordance with their own Terms and Conditions, suspended these domains. We call on eNom, UK2Group, Realtime Register, CentroHost and Moniker to clearly explain to the public why they will not do the same.