From: Derek Smythe [redacted]
Sent: 8/3/2018 7:15 AM
To: [redacted]
Cc [redacted]
Subject: Fwd: [redacted]]: Abuse complaint re: [redacted] closed

Dear Mr Marby and ICANN Complaints Office

Please note I do not accept this response from the ICANN Compliance office.

I clearly showed how the registrar does not check registration details as per the RAA 2013 WHOIS ACCURACY PROGRAM SPECIFICATION and is where the issues start, at DNS level. This is not addressed.

I clearly showed how the [redacted] contact system (webform and email) does not allow for accountability and performance metrics and this is abused. Ironically this is being used as an excuse here again for the second time in about 2 years in two separate ICANN Compliance Complaints where this is pointed out yet not addressed! I also gave an example of how [redacted] claims they did not receive a complaint, then mysteriously knows what the complaint is about.

I explained WHY this is not mere content issues, rather DNS abuse. yet we find the blanket "we are only a registrar" type response while allowing the DNS abuse to continue. This essentially says a Registrar is allowed to facilitate organized crime by self blinding to the obvious fake registration details and ignoring the RAA Accuracy Specification. This is not in line with other promises made and also not what was said to the European regulators.

This issue is NOT phishing on a hacked website or like. I also strongly suggest that ICANN SSAC be tasked to look at this DNS issue and similar. Simply put, many of these types of domains never have content and are used for emails in Advance Fee Fraud which is currently at an all time high (as statistics all around the world shows), is illegal in almost every country, yet depends on DNS abuse to succeed as shockingly spectacularly as it does. This leads to human rights issues. Many WIPO decisions are mistakenly made and won on phishing grounds whereas the underlying abuse is actually Advance Fee Fraud, something different. As such this issue should and must be taken seriously.

I even showed how [redacted] wins a UDRP, yet while this was ongoing, the respondent simply registers a replacement spoof of [redacted]. This makes a mockery of the UDRP system and subjects any such rights holder to perpetual victimhood at the whim of a malicious registrant - a $10 registration at a tolerant Registrar trumps a $2,500 UDRP every time as we see.

It cannot be denied that these oversights are not in line with stated and agreed upon ICANN policies and leads to gross harm. It is for this reason that I am now escalating this issue to the ICANN Complaints office as this is linked to another issue. Hopefully this can be turned into a learning opportunity.

Note: These responses are also being shared with various enforcement agencies and like in a confidential manner. I further also reserve the right to share this with the parties harmed or even publicly if needed, as the general public is also a victim to these oversights.

Regards,

Derek Smythe
Artists Against 419
[redacted]

-------- Forwarded Message --------
Subject: [redacted]]: Abuse complaint re: [redacted] closed
Date: Fri, 03 Aug 2018 10:31:29 +0000
From: Compliance Tickets [redacted]
Reply-To [redacted]
To [redacted]

Dear Derek Smythe,

Thank you for subm tt ng an Abuse comp a nt concern ng the reg strar [redacted]

[redacted]

Adm n Organ zat on:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

ATTACHMENT

[redacted]: Standards Compliance

ICANN Compliance complaint [redacted]

Derek Smythe

Artists Against 419

2018-03-17

[redacted] is an ICANN Accredited registrar that is bound by the ICANN RAA 2013:
https://www.icann.org/registrar-reports/accreditation-qualified-list.html

As such this registrar is obliged by the terms of the RAA.

This complaint opens up underlying systematic issues at the Registrar previously mentioned in ICANN Compliance Complaint [redacted]. This complaint was originally opened as Registrar Standard Compliance Complaint, changed to a WHOIS complaint by ICANN, ending with ICANN Compliance showing the registrar has complied. Yet the domain used for a bank spoof was still active and still spoofing the same bank with invalid registration data. This becomes more topical in the face of the GDPR.

Background

Most Advance Fee Fraud (AFF) activities use domains. Such domains are normally registered with proxies or deliberately supplied inaccurate registration details. Unlike phishing, domains are central to these activities and we even find continuous re-use of the same name by the same syndicate after suspension or lapsing.

It needs to be understood that this fraud could not be as effectively perpetuated without a domain. Such a domain is under malicious control. A hosting suspension will see such a domain merely rehosted, or even repurposed to such as the domain [redacted] which was on IP [redacted]. After suspension, it changed it's MX to [redacted] with no online content. Likewise the fraudster may even now use subdomains which are extremely difficult to detect. As such this is clearly not a mere content issue. A malicious party registers a domain with malicious intent. The domain has no other legitimate purpose for such a party other than the anticipated malicious usage.

Registrar [redacted] was found to be the sponsoring registrar with the second highest count of long lived malicious recorded by Artists Against 419 in 2017.See [redacted]

While Advance Fee Fraudsters continuously probe all registrars to try and obtain a foothold for their malicious activities which are illegal internationally, most registrars will promptly terminate such a domain where given evidence of such malicious activities, especially if linked to proxy abuse or fake registration data.

This is not the case with [redacted]. They believe any such domain usage not their responsibility.

This complaint address some of the issues where such malicious domains are registered at this Registrar and the lack in honouring of the RAA 2013 obligations, which in turn leads to massive consumer harm.

Issues at hand:

- Knowingly allowing an affiliate RAA violating proxy
- Registrar does not validate registration data.
- Registrar obligations
- Registrar reporting system does not allow for accountability metrics..

Knowingly allowing an affiliate RAA violating proxy

Please refer ICANN Compliance complaint ~[redacted]: Privacy/Proxy complaint. This complaint shows that emails to reseller [redacted] and Registrar [redacted] were sent and were acknowledged by the reseller. It shows that the proxy is mentioned that still violates the RAA 2013. This was never addressed.

The ICANN RAA obligates the sponsoring Registrar to ensure that their affiliates abide by the RAA. This never happened.

> *3.12 Obligations Related to Provision of Registrar Services by Third Parties. Registrar is responsible for the provision of Registrar Services for all Registered Names that Registrar sponsors being performed in compliance with this Agreement, regardless of whether the Registrar Services are provided by Registrar or a third party, including a Reseller. Registrar must enter into written agreements with all of its Resellers that enable Registrar to comply with and perform all of its obligations under this Agreement. In addition, Registrar must ensure that:*
>
> …
>
> > *3.12.4 Its Resellers comply with any ICANN-adopted Specification or Policy that establishes a program for accreditation of individuals or entities who provide proxy and privacy registration services (a "Proxy Accreditation Program"). Among other features, the Proxy Accreditation Program may require that: (i) proxy and privacy registration services may only be provided in respect of domain name registrations by individuals or entities Accredited by ICANN pursuant to such Proxy Accreditation Program; and (ii) Registrar shall prohibit Resellers from knowingly accepting registrations from any provider of proxy and privacy registration services that is not Accredited by ICANN pursuant the Proxy Accreditation Program. Until such time as the Proxy Accreditation Program is established, Registrar shall require Resellers to comply with the Specification on Privacy and Proxy Registrations attached hereto.*
> >
> > …
> >
> > *3.12.6 In the event Registrar learns that a Reseller is causing Registrar to be in breach of any of the provisions of this Agreement, Registrar shall take reasonable steps to enforce its agreement with such Reseller so as to cure and prevent further instances of non-compliance.*

Registrar does not validate registration data.

This issue is extremely topical at the dawn of the UDPR. In the current discussions on WHOIS data, the importance the thereof is discussed. In the latest ICANN published document on the issue at https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf we find (emphasis my own):

> **5.3.3. Accuracy of Registration Data (Pg12)**
>
> **Legal Analysis and Response to Community Comments**
>
> 5.3.3.4. The GDPR requires that personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay." In addition, it is important to note that compliance with local laws is expressed or implied in ICANN's agreements with contracted parties.
>
> 5.3.3.5. In principle this accuracy principle is similar in its scope and content to the accuracy principle

stated in currently applicable European data protection law27 and contemplated in the Registrar Accreditation Agreement. (The current Registrar Accreditation Agreement already includes accuracy requirements such as the validation and verification of some data elements, and the provision of notice to registrants about how to access, and if necessary rectify the data held about them.) Also, ICANN has other accuracy related initiatives such as WHOIS Accuracy Reporting System project. The GDPR therefore does not require the introduction of a new verification or validation requirements.

We need to ask what happens if a Registrar becomes aware of illegal activities where they are the sponsoring registry? More so, what happens when the registration data is patently and obviously bogus? This is issue also reflected in ICANN Advisory dated 3 Apr 2003, https://www.icann.org/news/advisory-2003-04-03-en

On the other hand, where a registrar encounters a severe Whois inaccuracy being exploited by a registrant to evade responsibility for fraudulent activity being carried out through use of the domain name, prompt action by the registrar is appropriate.

In the previous case we referred in regarding the massive [redacted] spoofs we saw patently fake registration data that easily seen. Please see a report, the [redacted] report, found here: [redacted]

These are essentially later evens after the earlier report and by the same party. This report shows one party using many bogus identities and telephone numbers to spoof banks and other business, establish fake non-existent business entities such as couriers and like. Extremely prominent is the [redacted] being continuously spoofed. In essence this is a continuation of the earlier complaint [redacted]. While this may be seen as "content issues", the analytics done on the registration data is not. This shows DNS abuse for fraudulent purposes.

Clearly this shows how this party has been the cause of direct losses to legitimate companies as well for UDRP costs, yet they are ineffective as the registrant uses the same bogus registration data to register a replacement malicious domain.

The analysis shows how one party is using telephone numbers that does not exist, where the same number has both UK and Nigerian prefixes. It shows how, despite having made [redacted] aware that [redacted] does not exist in Nigeria, these are still used. It shows non-existent 5 digit postal codes. Phone verification could not have succeeded, it would be impossible. Yet these details are continuously used. Essentially party is a [redacted]: Ref [redacted]

Ironically these details would put [redacted] in violation of the GDPR as well.

Apart from [redacted] above, we can look at registrations linked to email address [redacted] at [redacted]: [redacted]

Registrant Name: [redacted]
Registrant Organization:
Registrant Street: [redacted]
Registrant City: [redacted]
Registrant State/Province: [redacted]

Registrant Postal Code: [redacted]
Registrant Country: [redacted]
Registrant Phone: [redacted]
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: [redacted]

Obviously something is drastically wrong UK postal code as that is not the format for UK postal codes. Not obvious, is that [redacted] is 25 miles away from [redacted] (as [redacted] here). Yet the RAA 2013 states *"Validate that all postal address fields are consistent across fields (for example: street exists in city, city exists in state/province, city matches postal code) where such information is technically and commercially feasible for the applicable country or territory."*

This information is available and technical feasibility exists.

Something is obviously also drastically wrong with the telephone number format. Yet the ICANN RAA 2013 specifies *"Validate that telephone numbers are in the proper format according to the ITU-T E.164 notation for international telephone numbers (or its equivalents or successors)."* Correcting this number by removing the extra [redacted], we get [redacted]. But this is the telephone number of [redacted] UK?

The below snapshot is from [redacted], where this link is found on the official [redacted] website at [redacted]

It's clear this phone number was never properly validated.

Yet this fake set of registration details is used in advance fee fraud to spoof [redacted] also used to create fictitious couriers and other entities. These are all malicious domains. It is also no surprise that these domains originate at reseller [redacted], where more than 60% of the malicious domains attributable to [redacted] are registered.

We continuously see such obvious inaccurate registration data at this registrar. It would be impossible to make a list of all the domains seen to date which fails merest scrutiny and was not validated. One such example would be UK phone numbers being too short once "fixed" due to format issues, example domain [redacted]

In turn these lacking checks have been massively abused to register malicious domain that are being abused in consumer facing fraud.

Registrar obligations

Once a malicious domain has been detected, it is desirable that such a domain should be suspended or otherwise disabled as soon as possible. The harm is ongoing while it's active.

Ideally the ICANN reporting system should be used if possible, but this does not allow for rapid escalation. As such it's desirable rather to contact the sponsoring registrar directly. Theoretically this should not

matter. After all, the ICANN RAA WHOIS ACCURACY PROGRAM SPECIFICATION Par 4 mandates the registrar to investigate, the registrar Obligations 3.18 says:

3.18 Registrar's Abuse Contact and Duty to Investigate Reports of Abuse.

3.18.1 Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall publish an email address to receive such reports on the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.

3.18.2 Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.

3.18.3 Registrar shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports. Registrar shall document its receipt of and response to all such reports. Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice.

Looking at [redacted] web page, we find terms to be here: [redacted]. It says (emphasis my own):

Abuse Reporting Procedures

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

The abuse reporting form is at and says:

Report Abuse

This goes with the earlier statement made, the registrar considers all malicious domain issues to be content issues. This is an extreme disjoint from the realities of many fraud issues and in contradiction with issues such as botnets and Advance Fee Fraud where much of such is self-evident, even phishing where the registrant registers a domain for phishing. This is DNS abuse.

If this registrar cannot decide on obvious issues such as clear self-evident illegality, why did this registrar decide to become a registrar? After all, in the RAA 2013, we find:

> *1.13 "Illegal Activity" means conduct involving use of a Registered Name sponsored by Registrar that is prohibited by applicable law and/or exploitation of Registrar's domain name resolution or registration services in furtherance of conduct involving the use of a Registered Name sponsored by Registrar that is prohibited by applicable law.*

In fact, a registrar's accreditation may even be terminated:

> *5.5.2.1.3 with actual knowledge (or through gross negligence) permitted Illegal Activity in the registration or use of domain names or in the provision to Registrar by any Registered Name Holder of inaccurate Whois information; or*

This acknowledges the role the registrar should be playing.

AFF is predominantly domain based fraud. A malicious registrant registers a domain for malicious purposes, to defraud consumers. The domain has no legitimate purpose. It may be used to spoof a real company or not, that is incidental to the fraud. Relying merely on copyright and trademark issues does not address the issues consumers are facing nor would we have the rights to access those tools like the UDRP and URS mechanisms. Reporting such a domain to law enforcement results in the questions: Who is the victim, what was the loss, in which jurisdiction is your victim. Only if the victim is in the respective law enforcement's agency **and** if (collective) losses are great enough will they intervene. **This is after the fact and not consumer protection**. This would assume these incidents can be linked. Fake whois undermines this right. This leaves consumers in a quandary and allows the fraudsters to flourish. This is partially the reason why consumer fraud losses are also at an all-time high. The BBB study clearly showed what a devastating effect this had had on the consumer and the legitimate pet trade industry: https://www.bbb.org/puppyscamstudy/ - this is but merely the tip of the iceberg.

Further AFF also massively leads to privacy loss. The GDRP expects validation and accountability. Yet under the above circumstances the AFF make no attempt to even protect the consumer, instead defraud them, steal their identities in identity theft, extort them and abuse them in ways that are unthinkable. Many of the website trivially leak consumer data. There is zero respect for the victim in this fraud. An example would be the mentioned malicious [redacted] registrant with [redacted] phone number; domain [redacted]. Snapshot:

[redacted]

These details can be found in the clear with no protection.

The big issue with host suspension for a malicious domain is it offers zero mitigation relief and has no lasting value; the registrant is still in control of the domain by being in control of the DNS, ironically also mentioned in [redacted] services where they try to distance themselves from the issue. It's this reluctance to act, that has seen an exodus of Advance Fee Fraudsters from other registrars to [redacted] where they find sanctuary, resulting in them becoming the second most Advance Fee Fraud used registrar.

Registrar reporting system does not allow for accountability metrics

Emails to [redacted] results in no reply ever being received. Submissions via their web form do not result in an acknowledgement.

As was seen in the previous complaint against this registrar, they in fact denied ever receiving such notices. This begs the question: Is this ICANN accredited registrar actually abiding by the RAA 3.18.3 : "Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice.". Or are they filtering such records. Or is their system really losing messages. Best practice and metrics allows for acknowledgements which are trivially easy to implement.

This lead to one incident below where [redacted] of [redacted] and [redacted] of [redacted] are eventually included in frustration:

On 5/9/2017 2:40 PM, Derek Smythe wrote:

Hello [redacted]

I lodged a complaint via your web form a bit back on domain [redacted], since you absolutely insist your web forms be used.

No ticket or reply was ever received. Additionally this domain is still active as well despite showing the issues with this domain registration.

For the sake of accountability, may I please have a dated ticket reference and a copy of what was submitted?

Thanks.

Derek Smythe
Artists Against 419
[redacted]

On 2017-05-09 11:58 PM, [redacted] wrote:

Sorry, but we do not have purview over the content on web sites as we clearly state on our web site. You are advised to contact the host.

Thanks,

[redacted]
[redacted] support

On 5/9/2017 4:59 PM, Derek Smythe wrote:
[redacted]

I pointed out fake registration details in the ticket ?!!

I once again pointed out this in this request:
despite showing the issues with this domain registration.

But it's fine. I've done a pretty good reconstruction and summary. It also prompted me to question what is actually happening here and is wrong with your reply.

This now becomes an ICANN community issue. I'll once again explain the problematic registration details.

I'll copy you on it, also ICANN compliance as I've already shown them why your form usage is form abuse in the past, despite their unwillingness to address it.

Derek

On 2017-05-10 02:35 AM, [redacted] wrote:
Derek,

Sounds great - have a fantastic evening. Also, for you edification, the WHOIS details reflect usage of our privacy service, so, despite your claims, there are no problems with the WHOIS registration details.

We advise you to read our abuse reporting procedures in full and please do not make frivolous reports of data that clearly has no problems. It wastes our time, as well as everybody's time that you bring into your baseless complaint.

Thanks,

[redacted]
[redacted] support

On 5/9/2017 7:13 PM, Derek Smythe wrote:
Cc: [redacted] & ICANN Compliance

No problem [redacted]

I simply asked for a copy of an original complaint since you did not respond to it. You replied that you have no purview over content of websites. Not exactly what I asked, is it?

Your extreme concern in ensuring a safe accountable internet is also noted. Also how you view your proxy services as a shield for a known bad apple.

Since it seems you are a bit "slow at joining the dots":

Your hidden registrant is a fake entity and the domain is malicious.

To explain the term malicious domain: A domain purposely registered by a malicious party for associated malicious usage, is malicious.

We've been tracking it before it moved to you:
[redacted]

Look at the name server and make a note of it:
> Name Server: [redacted]
> Name Server: [redacted]

Look at his other domain, which he incidentally reported himself - yes, it is a "he" and yes it is the same party: [redacted]

Once again note the nameserver:
>Name Server: [redacted]
> Name Server: [redacted]

Please do not believe the bank details you see on the second domain cocaine domain ... they may belong to an innocent party. Please ask the US Dept of Homeland Security if you require more details since you claim to be US based. I can put you in touch with them if required.

Look at the whois details of [redacted]

This email serves as a notice that you were informed of the nature of domain [redacted] using the [redacted]. As such ICANN RAA 3.7.7.3 applies. I trust [redacted] will accept the responsibility as promised.

Additionally you now also know about domain [redacted] claiming to be selling cociane in the USA. Naturally selling cocaine is illegal in the USA. You are the sponsoring registrar for this domain.
> Domain Name: [redacted]
> Registry Domain ID: [redacted]
> Registrar WHOIS Server: [redacted]
> Registrar URL: https://[redacted]
> Updated Date: 2017-05-03
> Creation Date: 2017-04-19
> Registrar Registration Expiration Date: 2018-04-19
> Registrar: [redacted]
> Registrar IANA ID: [redacted]
> Registrar Abuse Contact Email: [redacted]
> Registrar Abuse Contact Phone: [redacted]

To insure your unaccountable system becomes semi-accountable, I request [redacted] and [redacted] please also submit this email via the [redacted] form at [redacted] which should serve as evidence of such an alert being submitted to [redacted]

Have a marvelous day!

Derek

Subject: Re: [redacted] (add [redacted])
Date: Tue, 9 May 2017 20:01:17 -0700
From: [redacted]
To: [redacted]
CC: [redacted] at [redacted] [redacted], compliance@icann.org <compliance@icann.org>

We never received any abuse report filed via our web site form for the domain you listed ([redacted]).

My concern is for following our abuse reporting guidelines as that ensures that we are able to process, review and consider abuse reports. However, as noted above, no form was ever submitted on our site. Further, your assertion that the Registrant is a "fake entity" is not something you are in a position to state as the Registrant information has always been shielded via our privacy service while the domain has been registered with us.

If you want to file a proper abuse report, we recommend you do so via our online form, not via your email below.

Thanks,

[redacted]

[redacted] support

Ironically [redacted] knew about the “content issue”, despite not seeing the complaint?

Header for last email:

```
Return-Path: [redacted]
Delivered-To: [redacted]
Received: [redacted]
```

The issue here was that the domain was registered at [redacted], along with numerous sibling domains. These claimed to be selling anything from marijuana to hard drugs such as cocaine, heroin, also suicide drugs such as Euthasol. These all abused Registrar [redacted]s proxy service. When [redacted] was alerted, they first revoked their proxy, the registration details were fake, then they started terminating them. During this last step the registrant moved some of the domains to [redacted]. The registrant is a well-known malicious actor who spams his drug domains on online forums. One such was even on our own forums. Using DNS elements it is possible to trace this party.

Despite [redacted], [redacted] and I having also reported this to [redacted] proxy, no details as per ICANN RAA 3.7.7.3 were ever received.

These domains are Cameroonian in origin (see whois of mentioned [redacted]) and are commonly also associated with extortion after fraud on cancer patients.
Ref: [redacted]
Ref: [redacted]

It’s no surprise to find the same domain (not ICANN regulated) [redacted] now used for a pet scam. Indeed, this ties in with issues also mentioned in Mr [redacted] report in pet-scam fraud. Pet scams are the tip of this iceberg, ill-defined and massive domain abuse, originating from the Cameroon.

It's this situation that is currently developing and growing at [redacted] Consider just one of this party's identities, [redacted] : [redacted]
(Feel free to follow the name and dig deeper, returning to the start and more fake identities)

Essentially this makes a mockery of RAA compliance as mentioned in the GDPR discussions and ties up with the earlier mentioned problematic WHOIS issues.

Another example: Submitted via both webform and email No response. Domain is still active.

Subject: Reported via form: [redacted]
Date: Sun, 10 Sep 2017 01:26:18 +0200
From: Derek Smythe [redacted]
Reply-To: [redacted]
Organization: [redacted]
To: [redacted]
CC: [redacted]

Hello [redacted]

The following has just been reported via your online abuse form.
Dropping a mail here since i know from history your form does not always work.

Domain Name: [redacted]
Desired Resolution: Deactivate Domain

Details:
Fake phrama

Claims to sell LSD and other schedule drugs

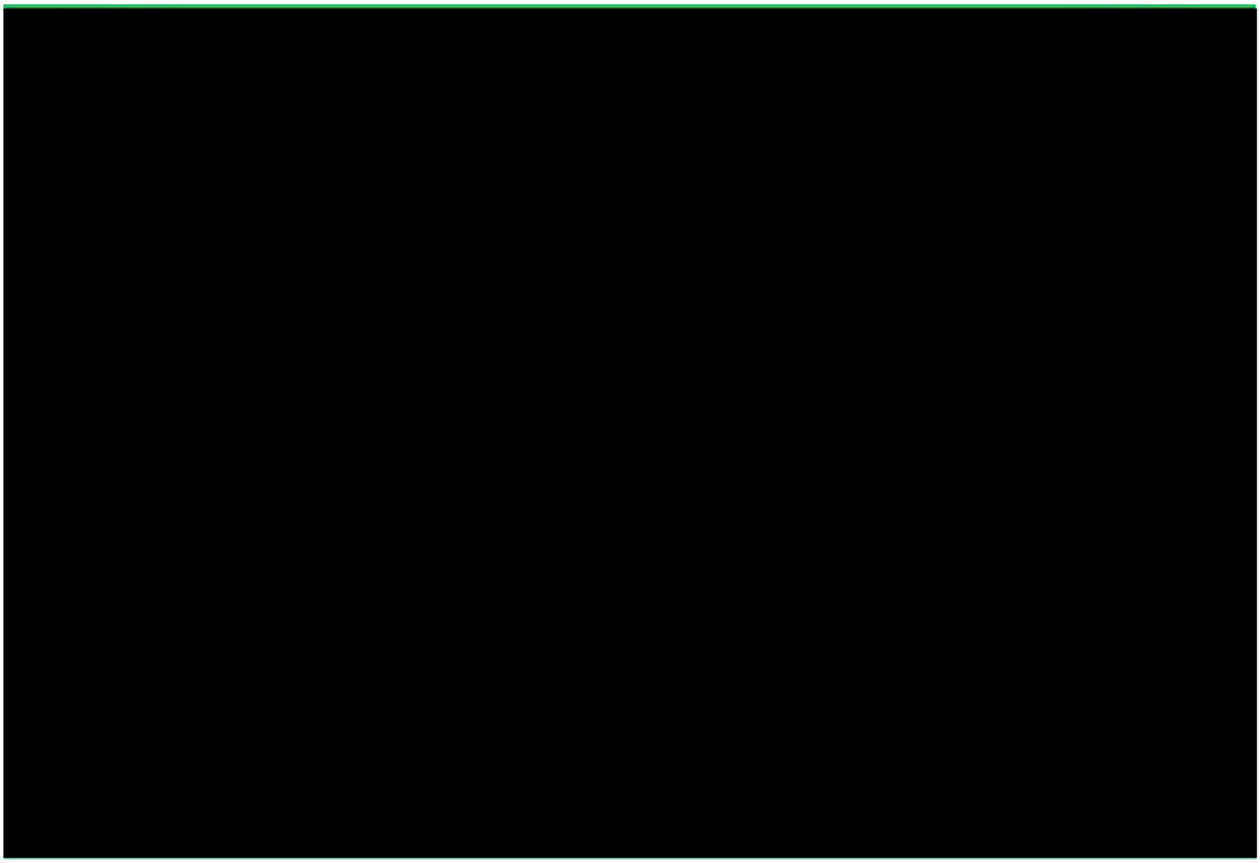
[redacted]

Credit card details theft:
[redacted]

Ref:
[redacted]

Derek Smythe
Artists Against 419
[redacted]

[redacted] were copied and listed this:
[redacted]



It is common cause that LSD is illegal in the USA. However, what we are seeing here is an attempt at claiming to sell the drug, but having no access to it. In turn this leads to extortion typically via bogus couriers claiming to do “discrete” shipping.

We also see the attempted credit card details theft. This is a self-sustaining caustic environment also funding further domain purchases. This leads to massive consume harm.

[redacted]

Conclusion

Despite this registrar being ICANN accredited, they do not uphold the norms of the ICANN RAA.

We see this in the way proxies are used at their reseller. We see this in the lacking quality of registration data. We see them massively abused by criminal syndicates, abusing malicious domains for advance fee fraud, as a bullet-proof registrar. These syndicates know fake registration details will shield them. They also know the authorities can impossibly investigate each and every issue.

The registrar feels themselves absolved from any responsibility in this issue and are happy to facilitate the trade in malicious domains. In turn this creates an environment where there is a lack of confidence to report serious issues to them.

This leads to gross ongoing fraud and consumer harm in self-evident illegality.

---ooo000ooo---