OTA
Online Trust Alliance

CLOUD SERVICES ONBOARDING RISK EVALUATION FRAMEWORK

Released October 1, 2013

This document is a recommended best practice and resources for Email Service Providers (ESPs), hosters and data centers to help identify common risk factors when accepting a new account, agency or reseller. Onboarding and vetting new customers is increasingly becoming a challenge for cloud, infrastructure and marketing service providers. Growing numbers of cybercriminals and deceptive businesses are trying to gain access to legitimate services to deploy attacks including, spam, DDos attacks, click fraud and other purposes. While these efforts can be detected and blocked within 24 hours of being deployed, the damage has been done and the spammer or cybercriminal will just move to another unsuspecting service provider willing to accept their business.

The challenge for service providers is to provide an efficient service to legitimate customers with a vetting process to quickly detect fraud. This includes not only new accounts but also increasing capacity and bandwidth of existing accounts who may have been inactive or low volume while planning a large scale exploit.

Detection of fraudulent and malicious intent is critical to not only the ability to monetize and be paid for the services, but more importantly the resulting reputation harm which may occur. This often impacts the service provider, clients and ultimately the end user who has been compromised by the malicious email, deceptive web site and related exploits. The resulting damage is not only to the users or organizations targeted, but also to other customers of the service provider and others who may share an IP range or virtual server, causing collateral damage. This may result in having mail throttled by ISPs, sites blocked and listing on black lists by the anti-spam and phishing communities. In addition, service providers need to aware of the risk of potential legal and regulatory actions, by failing to take reasonable steps to protect users from harm.

When implemented, the framework can help to prevent acceptance of customers with fraudulent and malicious intent. This effort leverages the framework developed by the advertising community to detect and identify malicious advertisers.[1] As implemented today, OTA encourages sharing of such known bad actors which this framework identifies to help stem the “waterfall effect” of bad actors jumping from one service provider to another.

[1] https://otalliance.org/malvertising.html

In reviewing the framework it is important to note that not all questions listed are appropriate for every ESP or hoster. The risk thresholds for some of the questions need to be set by each service provider based on their respective industry and services being rendered. It is expected service providers will customize this list to create their own vetting program helping to assess a company's acceptable risk level for onboarding new accounts. Several EPSs and hosters who contributed to this document have subsequently created client profiles based on their specific markets and risk factors.[2]

Other consideration is the acceptance of high risk clients such as those selling stock tips, gambling, pharmaceuticals, herbal supplements and others products. It is suggested that service providers consider adding language in the terms of use, outlining business practices which might be unacceptable. For clients with a moderate risk, it is recommended service providers throttle daily volumes of mail and server capacity. Over time, based on reporting from major ISPs and others, capacity can be raised for clients with no history or pattern of abuse or complaints.

How to use this form

Evaluate the risk factors in each of the following risk areas balanced against your organization's risk tolerance level and procedures:

1. Domain reputation
2. Past complaints
3. Timing and Urgency
4. Corporate Identity
5. Individual Identity
6. Data Use

Determining Risk / Risk Tolerance

Determining levels of acceptable risk can vary greatly based on individual company and service offerings. This form will not make a decision for you or your company, but is designed to help provide visibility to better understand the level of risk and business decisions and when additional information or investigation may be required. This framework is based on best practices from a broad range of stakeholders, and is provided for informational purposes only. Companies may wish to develop scoring mechanisms and thresholds for flagging risk based on their own business model, legal environment and risk tolerance. New accounts, partners and resellers who yield multiple cautionary scores, may warrant ongoing monitoring and throttling of services.

[2] Other industry organizations have developed materials to address some of the related issues discussed. Readers may wish to visit the Email Service & Provider Coalition http://www.espcoalition.org/ as well as MAAWG http://www.maawg.org/sites/maawg/files/news/MAAWG_Vetting_BCP_2011-11.pdf.

It is recognized early stage or startup mailers, sites and reseller may receive cautionary scores based on their ramp-up and maturity. These scores by themselves do not necessarily indicate a high risk, and should be monitored and throttled until a history of good behavior can be established.

For each of the risk areas, inert a "0" for low risk, "2" for medium and a "4" for high risks. Accounts with a low score are generally considered a low risk, while sites with a high score may require additional investigation before being accepted. While all attributes are currently weighed equally, users may wish to modify scoring based on the impact to their respective business.

Mailers and sites that are determined to be malicious or fraudulent should be reported to abuse desks of ad networks and working groups. OTA recommends sharing of this information with other trusted parties and partners. This is important as fraudsters often attempt to compromise multiple parties concurrently and such sharing may enhance overall protection of the ecosystem. In especially grievous discoveries, you may want to consider contacting law enforcement. In addition, sites or advertisers who are believed to be mis-representing another brand or "brand jacking" should be forwarded to the respective brand owners.

Last but not least, companies need to develop a policy on what should be communicated back to prospective accounts that are not being accepted. It is recommended that users of this form complete a legal review and considering adding that the acceptance of customers is subject to a review including, but not limited, to credit reports, reputational and third party data.

This document reflects strategic input and guidance from a broad cross section of OTA members including but not limited to Act-On Software, Agari, American Greetings Interactive, Constant Contact, eDialog, Epsilon, Exact Target, eWayDirect, Harland Clarke Digital, Iconix, LashBack, Listrak, Marketo, Microsoft, Responsys, Return Path, Sailthru, SilverPop, Symantec, TrustSphere, Twitter, ZEDO and Zynga.

OTA welcomes feedback, additional criteria and considerations. To submit suggestions and comments, please email admin@otalliance.org. Updates to this form and resources are published at https://otalliance.org/resources/

Material in this publication is for educational and informational purposes only. Neither the publisher, the Online Trust Alliance (OTA), its members nor the authors assume any liability for any errors or omissions nor how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. OTA makes no assertions or endorsements regarding the security or business practices of companies who may choose to adopt such recommendations outlined. For legal or other advice, please consult your attorney or other appropriate professional. The views expressed in this publication do not necessarily reflect the views of OTA member companies or affiliated organizations.

OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

OTA
Online Trust Alliance

New Account Risk Evaluation

Date: ______________________

Company Name: ____

Website: ____

IP Addresses: ____

Contact Name(s): ____

Phone: _________________________ **Email Address:**__________________

Domain:____

Products / Services: ____

Assessment Conducted by: _______________________________________

Referral / References: ____

____

Other Comments (why are they changing providers): ___________________

____

____

____

____

New Account Risk Evaluation – Check List

	Low Risk (0)	Caution (2)	High Risk (4)
1. Domain Risk Factors			
a. Age – How long has the domain been registered?[3]	**> 12 months**	**6-12 months**	**< 6 months**
b. Activity – How active has the domain or IP been over the last 90 days?[4]	Consistent activity		No activity
c. Has the domain been recently transferred to or from a 3rd party?	No	Unknown	Yes
d. Is the "Who Is" registration private or by proxy?	No	Unknown	Yes
e. Does the country TLD code match the address of the customer contact information?	Yes	Unknown	No
f. Does the site have a physical address that can be validated? [5]	Yes	Unknown	No
g. Does the corporate domain utilize SPF, DKIM & DMARC for their TLD and subdomains?	Yes		No
2. Reputation Risk Factors			
a. Has the company or contact ever been blocked by a third party anti-abuse or anti-spam organization? [6]	No	Unknown	Yes
b. Validate the forecasted daily traffic or volumes, are they realistic?	Yes	Unknown	No
c. Can you check their reputation with previous service provider? [6], [7]	Yes		No
d. Do they frequently change service providers?	No		Yes
e. Is the company in a known vertical that has historically been exploited by bad actors? (At risk segments include nutraceuticals, payday loans, stock tips, security, anti-virus products or solutions).	No	Unknown	Yes [8]

[3] Check using the Who Is database look up. Many registrars offer tools http://www.networksolutions.com/whois/index.jsp.

[4] Domains are often registered months in advance of being used for an exploit. Look at past traffic history include large spikes after no activity.

[5] Check address using Google Maps / Street view or other similar services.

[6] Sources such as Senderbase (Cisco) http://www.senderbase.org/home, Spamhaus http://www.spamhaus.org/ and SenderScore https://www.senderscore.org/ (ReturnPath) and others should be considered when evaluating a company's past reputation

[7] Consider reputation sources cited above as well as others such as TRUSTe http://www.truste.com & the Better Business Bureau. http://www.bbb.org/us/bbb-online-business/

[8] Security warnings from fake anti-virus companies or discounted software offers have been a common exploit.

	Low Risk (0)	Caution (2)	High Risk (4)
3. Timing and Urgency Risk Factors			
a. Is the account creation a last minute order or right before a holiday?	No		Yes
b. Is the order inbound and unsolicited?	No		Yes
c. Is the order prepaid?	No		Yes
d. Are they willing to pay for services not typically requested?	No		Yes
4. Corporate & Website Risk Factors			
a. Do they have a DUNS number? [9]	Yes		No
b. Does the website appear to be unprofessional or have multiple obvious errors? [10]	No		Yes
c. Does the site have an insecure SSL connection, mis-matched SSL certificate or expired SSL certificate? [11] [12]	No		Yes [13]
d. Does the site have malware or known exploits?[14]	No		Yes
e. Does the site list corporate officers and bios which can be validated via other sites?	Yes		No
5. Individual Risk Factors (customer contact)			
a. Few or no industry contacts, references or search data	No		Yes
b. Can you validate the identity of the contact?	Yes		No
c. Does the email address (domain) correspond to corporate site? (Both the from and reply email addresses)?[15]	Yes		No
d. Does the reply email address bounce?	No		Yes

[9] http://en.wikipedia.org/wiki/DUNS_NUMBER

[10] Check for quality graphics, spelling, does it appear to be scraped from another site? Check page URLs, do they point back to the same domain.

[11] Easy site check using SSL Labs serve test tool https://www.ssllabs.com/ssltest/index.html.

[12] Sites with an F score from SSL Labs, should be evaluated.

[14] Consider using site canners from companies such as SiteLock, RiskIQ and / or Symantec.

[15] Note there are legitimate instances where a domain may not match a company where as there may be a corporate email domain or a domain of a parent company. For example the Wall Street Journal (wsj.com) is a Dow Jones Company, (dj.com) and a contact may be from a parent domain represent a wholly owned brand, division or subsidiary.

	Low Risk (0)	Caution (2)	High Risk (4)
6. Data Use, Privacy & Email Practices			
a. Is their data and name acquisition strategy and practices consistent with industry norms and self-regulatory best practices.	Yes		No
b. Does the prospect share lists and or data with third parties including partners, advertisers or other brands?	No		Yes
c. Do they send email on behalf of partners or third parties?	NO		Yes
d. Do they engage in affiliate marketing or operate their own affiliate program?	No	Yes	Yes
e. Does the data use and privacy policy reflect the above?	Yes		No
f. Is the privacy policy discoverable on the home page of the site?	Yes		No
g. Have they implemented SPF & DKIM for their outbound email, (corporate and marketing domains / subdomains)? [16]	Yes	No	No
h. Have they implemented DMARC? [17]	Yes		
i. Does their site participate in any privacy self-regulatory programs?	Yes		
j. Are they members of industry organizations which promote best practices, transparency and accountability? [18]	Yes		No
Total			

[16] https://otalliance.org/resources/authentication/index.html

[17] https://otalliance.org/resources/authentication/dmarc.html

[18] Such organizations include MAAWG, ESPC, OTA and others.