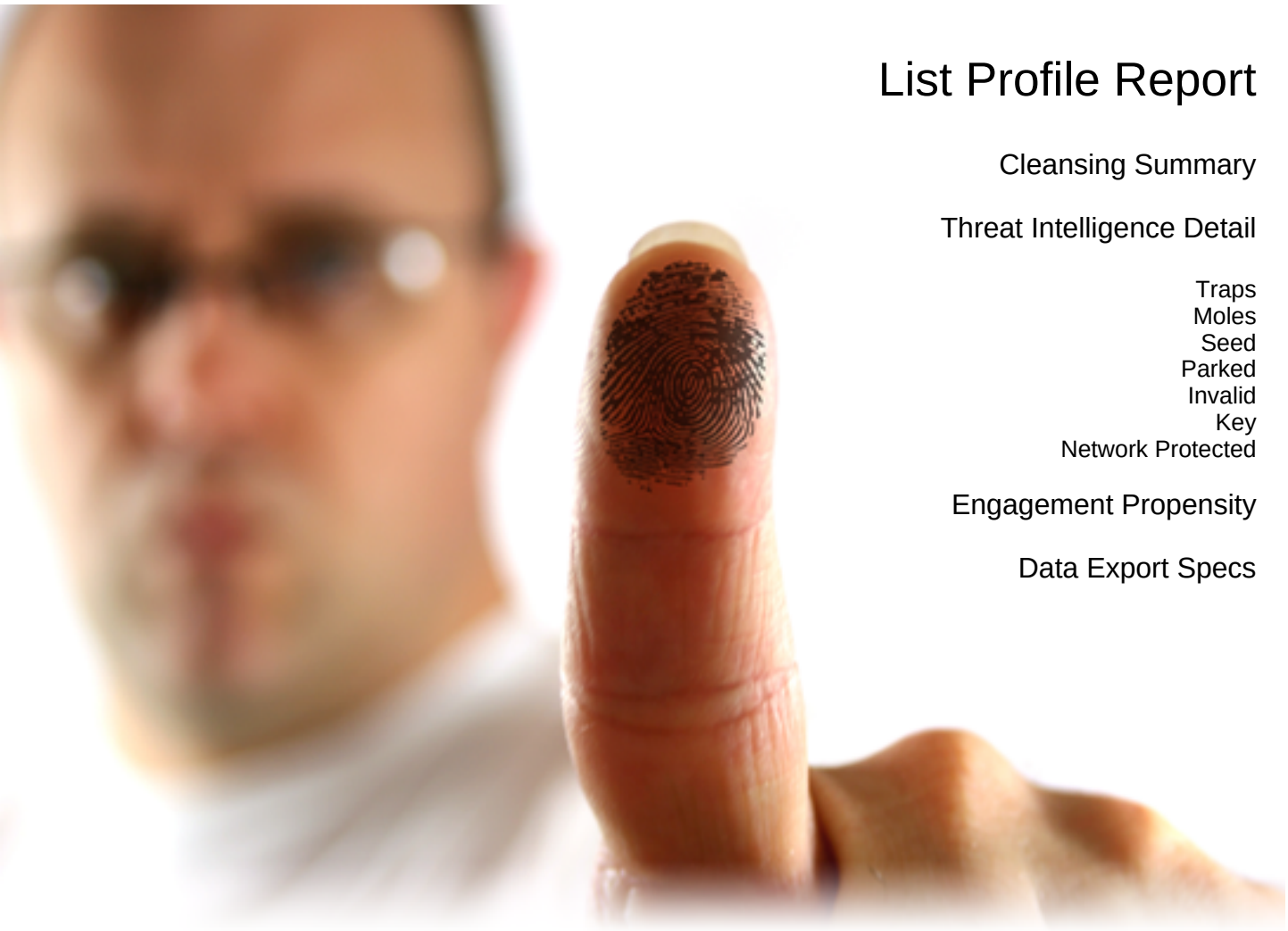
proshark



List Profile Report

Cleansing Summary

Threat Intelligence Detail

Traps
Moles
Seed
Parked
Invalid
Key
Network Protected

Engagement Propensity

Data Export Specs

File Name:

Sample List

Report Date:

June 04, 2017

Now it is time to **Let the results speak for themselves!**

proshark

Cleansing Summary

		Domain Count	Recipient Count
	Raw File. Raw file counts with duplicate entries removed.	**5,901** *(0)*	**8,614** *(100.0%)*
✅	**Certified Domestic.** US-based email address with no known reason to expect a delivery failure or harm to email senders online reputation.	**2,811**	**5,275** *(61.2%)*
✅	**Certified International.** Non-US-based email address with no known reason to expect a delivery failure or harm to email senders online reputation.	**12**	**13** *(.2%)*
❓	**Network Protected.** Managed SMTP filtering applications known to be highly collaborative, notifications sent to leading DNSBL sites in real-time.	**27**	**34** *(.4%)*
❓	**Key.** Complex pattern recognition and threat string algorithms designed to remove intra-domain recipients employed by that domain for use as spam traps.	**3,132**	**3,171** *(36.8%)*
❓	**Quarantine.** Once active traps gone dormant may become reactivated during a 90 day period. Yet actively considered certified.	**38**	**44** *(.5%)*
⚠	**Parked Site.** Email addresses that after careful evaluation have been established to be least likely to be responsive or engage.	**23**	**26** *(.3%)*
⚠	**Seed.** Third party oversight email address used for general monitoring of company's network resources. Removal of litigators and collaborative anti-spam activists historically known to purposely seed their email address(es) for the purpose of litigation.	**0**	**0** *(.0%)*
⚠	**Invalid.** Defined as the inability to actually deliver an email message to intended recipient's receiving domain per RFC standards.	**18**	**22** *(.3%)*
⚠	**Mole.** Collaborating recipient submission-based or domain-level, anti-spam solution with no current, direct ownership of resources involved. Yet historical evidence firmly establishes a relationship to one or more DNSBL sites.	**19**	**21** *(.2%)*
⚠	**Trap.** Purpose-built, Spam-trap, or Honeypot e-mail address, any e-mail messages sent to this address are immediately considered unsolicited. Email address has known association of having direct ownership or control over the resources involved with the reception of a message leading to its submission to one or more DNSBL sites.	**7**	**8** *(.1%)*

Recommended Usage Guidance

The guidelines presented below will ensure you are adhering to email best practices, enabling more emails to reach the inbox. As a result, you will mitigate any risk associated with emailing to potentially “bad” addresses and you will experience additional opens, higher click through rates, increased conversions, and more revenue while protecting your online reputation.

Safe to Send

Send **ONLY** if Recipient was organically acquired with user-based submission evidence OR has purchase activity within last 90 days *(open/click activity excluded)*

Do Not Send

Threat Intelligence Classification

Impressionwise’s data intelligence platform is based on policy-driven rule sets and real-time scanning algorithms that use a multi-layered approach to **identify**, **validate** and **protect** against a wide range of e-mail-based threats. These threats, ranging in severity, are broken down into the following categories for flexibility in customized export usage options while providing unprecedented, detailed insight.

Traps and Quarantine

Trap. Purpose-built, Spam-trap, or Honeypot e-mail address, any e-mail messages sent to this address are immediately considered unsolicited. Email address has known association of having direct ownership or control over the resources involved with the reception of a message leading to its submission to one or more DNSBL sites.

Quarantine. Once active traps gone dormant may become reactivated during a 90 day period. Yet actively considered certified. Quarantined values shown below in ( ).

DNE Elements Description	Active Domains (Quaran)	Active Recip (Quaran)
AB.SURBL.org URIBL	0	0
Abuse.ch Swiss Security Network	0	0
Abuseat.org (CBL) RBL	0	0

DNE Elements Description	Active Domains (Quaran)	Active Recip (Quaran)
Abusix RBL	0	0
AHBL.org RBL	0	0
Backscatterer.org RBL	0	0
Barracuda RBL	0	0
BBFH RBL	0 (1)	0 (1)
BBQ RBL	0	0
BlakJak RBL	0	0
Burnt-Tech DNSBL	0	0
CanTV DNSBL	0	0
CASA RBL	0	0
Choon RBL	0	0
ClickBot DNE	0	0
Cloudmark Anti-Spam Network DNE	0	0
Cyberlogic DNSBL	0	0
Cymru Bogon DNSBL	0	0
Cyveillance Threat Intelligence Network	0	0
D. D. N. S. B. L. RBL	0	0
Day Old Bread-SupportIntelligence.com URIBL	0	0
DeadBeef RBL	0	0
DNSBL	0	0
dnsbl.othello.ch DNSBL	0	0
DNSBLChile RBL	0	0
DRBL	0	0
DSBL.org RBL	0	0
Dynamic Domain Name Spoofers RBL	0	0
eBlockade.com RBL	0	0
EFnet RBL	0	0
Emailbasura DNSBL	0	0
Fail2Ban/ Blocklist.de Reporting Service RBL	4	5
FiveTenOther RBL	0	0
FusionZero RBL	0	0
General Quarantine	0	0
HostsControl DNSBL	0	0
IBM DNS Blacklist	0	0
Intercept DNS RBL	0	0
Internet Defence Systems RBL	0	0
Interserver DNSBL	0	0
Invaluement RBL	0 (8)	0 (9)

DNE Elements Description	Active Domains (Quaran)	Active Recip (Quaran)
iX RBL	0	0
JIPPGs RBL Project	0	0
JP.SURBL.org URIBL (user app net not incld)	0	0
Karmasphere RBL	0	0
Kempt.net RBL	0	0
KISA-RBL	0	0
Known Network Cable DNE	0	0
MailPolice.com RBL	3 (16)	3 (16)
MailSpike RBL	0	0
MainSleaze SpamBouncer RBL	0	0
Mobile Device FTC DNE	0	0
MXRate RBL	0	0
NiX Spam DNSBL	0	0
NJABL.org RBL	0	0
No-More-Funn RBL	0	0
NoSolicitado.org	0	0
NoToSpam.com	0	0
NSZones URIBL	0	0
Nukesapm.org RBL	0	0
ORBITrbl RBL	0	0
Passive Spam Block List	0	0
Pedantic RBL	0	0
Polar Communictions RBL	0	0
PowerWeb DNSBL	0	0
Project Honey Pot (http:BL) RBL	0	0
Quorum Listing Service	0	0
Redhawk RBL	0	0
RFC-Ignorant RBL	0	0
Rhyolite-DCC Checksum DNSBL	0	0
S5H RBL	0	0
Scientific Spam RBL	0	0
Shlink URI-RBL	0	0
Solid Clues RBL	0	0
SORBS.net-BBFH.org RBL	0	0
South Korean Network RBL	0	0
Spamblock DNSBL	0	0
Spambulance RBL	0	0
SpamCannibal RBL	0 (4)	0 (7)

DNE Elements Description	Active Domains (Quaran)	Active Recip (Quaran)
SpamChampuru DNSBL	0	0
SpamCop RBL	0	0
SpamEatingMonkey.net RBL	0	0
Spamgrouper.com	0	0
Spamhaus Contributing Partners	0	0
Spamhaus DBL URI-RBL	0	0
SpamHaus RBL	0	0
SpamLab RBL	0 (5)	0 (7)
SpamRats.com RBL	0	0
SpamStinks Anti-Spam	0	0
StopSpam.org RBL	0	0
SURBL.org URI-RBL	0	0
Technovision Spamsource RBL	0	0
Tiopan Consulting RBL	0	0
Toasted Spam	0	0
TornevallNET DNSBL	0	0
TRBL DNSBL	0	0
TRIUMF.ca DNSBL	0	0
UCE Protect RBL	0	0
Unspam Technologies	0	0
Unsubscribe Blacklist (UBL) RBL	0	0
URIBL.org URI-RBL	0	0
V4BL RBL	0	0
Webequipped DNSBL	0	0
WPBL (Weighted Private Block List) RBL	0	0
WS.SURBL.org URIBL	0	0
ZapBL DNSBL	0	0
Zenon.net RBL	0	0
ZoneEdit combined DNSBL	0	0

Moles and Dormant Accounts

Mole. Knowing or un-knowing collaborating recipient providing submission-based evidence manually or via automated, domain-level, anti-spam solution with no current, direct ownership of resources involved with the acquisition and processing of this email leading to its submission to a DNSBL. Yet historical evidence firmly establishes a relationship to one or more DNSBL sites.

proshark

DNE Elements Description	Active Domains (Quaran)	Active Recip (Quaran)
Abuse.ro URIBL	0	0
Barracuda Contributing Network	9	9
Bounce.io Seed Network	0	0
Clean-MX Anti-Spam Mole Network RBL	0	0
Cloudmark Contributing Network	0	0
Commtouch Anti-Spam Network DNE	4 (1)	4 (1)
DCC-Rhyolite Contributing Network	0	0
General Spamtrap Contributing Network	0	0
HostKarma RBL	0	0
Invalument Contributing Network	0	0
MailPolice Contributing Network	0	0
MaySoft SpamSentinel DNE	0	0
NJABL.org Network Mole	0	0
NSZones URIBL	0	0
OB.SURBL.org Anti-Spam Network DNE	0	0
Othello.ch DNSBL	0	0
Redcondor Anti-Spam Network DNE	2	3
ReturnPath Contributing Network	0	0
SORBS Contributing Network	0	0
SpamCop Mole	0	0
SpamCop Network Mole	0	0
SpamHaus Network Mole	0	0
SURBL Contributing Network	0	0
SURBL JP (jwSpamSpy + Prolocation)	0	0
SURBL OB (Outblaze)	0	0
SURBL PH (Phishing/ Malware Site)	0	0
SURBL SC (SpamCop/Spamvertised Site)	0	0
SURBL WS (Bill Stearns' SpamAssassin)	0	0
TrendMicro Contributing Network	3	4
UCE Protect Network Mole	0 (1)	0 (1)
Unspam Technologies RBL	1 (2)	1 (2)
URIBL Contributing Network Moles	0	0
Websense Anti-Spam Network DNE	0	0

Dormant Accounts. Email addresses are not permanent. When there has been no login activity for a long period of time, the recipient account is defined by the provider as “inactive” and turned into a form of unknowing collaborator with no non-delivery report (NDR) indicating “no such user” or “mailbox not found” being sent as a response. Thus any email sent during this period of time before account deactivation is assumed, in the collective, as spam and its email signature mapped and used to block any email to other active recipient accounts within the domain.

Provider Description	Domain Count	Recipient Count
AOL Invalid	0	0
Gmail Invalid	0	0
Hotmail, MSN, Live, Outlook	3	7
Yahoo Invalid	0	0

Seeds

Specifically defined as a, third party oversight email address used for general monitoring of company and company's network resources used. Also this category includes, litigious address removal – removal of litigators and collaborative anti-spam activists historically known to purposely seed their email address(es) for the purpose of litigation.

DNE Elements Description	Active Domains (Quaran)	Active Recip (Quaran)
General Monitoring Seed	0	0
Habitual Domain Protestors	0	0
Habitual Recipient Protestors	0	0
LashBack Seed	0	0
Litigious/ Anti-Spam Activist Seed	0	0
Phish Labs Cybercrime Intelligence	0	0
Returnpath.net-Sendercore Seed	0	0

Parked Site Intelligence

Defined as the registration of a domain name without using it for services such as e-mail or a website i.e. you would never receive a response to any emails sent to this domain.

Parked site intelligence gives you the leverage of avoiding sending email traffic to millions of unused and parked website domains. Since parked domains have previously not been configured for email, any recipient is by definition, invalid and being spammed. This creates an instant, rich, and magnanimous source of pristine spam trap data. The information contained from messages sent to these sites has shown a great propensity to be utilized by anti-spam solution providers and other RBL networks as essentially the world's largest global and organic honeypot spam trap network.

Sender's also have the added value of higher engagement by suppressing these sites from your mailing list, as the email addresses associated with these sites has been established to be unlikely to be responsive or engage.

Identified Elements Description	Domain Count	Recipient Count
Domain Actively Advertised For Sale/CyberSquating	4	5
Domain Pending Renewal or Deletion	1	1
Domain Suspended or Expired	6	6
Parked Domain	6	7
Parked Site	6	7

Address Validation

Once first tiered DNE (do not email) elements (traps, moles, parked sites, etc.) have been removed the second greatest threat to your message deliverability and eReputation is bounced addresses. Bounces come in many forms some temporal (mail box full, etc.) while others are permanent notifications (mailbox) not found, etc.) Even if you have a trap-free or “clean” list sending to bounced email addresses can cause great harm as most large ISP’s (AOL, Yahoo, Gmail, Hotmail, etc.) use this information in the form of a bounce rate to determine whether or not to accept any future mail from your sending domain.

Domain Level Checks

DNS Validation: Defined as the inability to actually deliver an email message to intended recipient, receiving domain per RFC standards at the time the data cleansing scan was performed.

Domain Origination (Domestic vs International): Sourced from IANA’s database of TLD extensions and Regional Internet Registries (AfriNIC, APNIC, ARIN, LACNIC, RIPE). Assessment is based off the geographic location of the originating IP that the MX record.

Blackhole Identification: A blackhole e-mail address is an e-mail address which is valid (messages sent to it will not generate errors), but to which all messages sent are automatically deleted, and never stored or seen by a real person.

Invalid Elements Description	Domain Count	Recipient Count
Failed Domain DNS Validation	10	10
Invalid Recipient	0	0
Malformed DomainName	0	0
Malformed Recipient Address	0	0
No Domain MX Record Present	5	5
Non Responsive Domain MX	0	0
Null MX/ Domain Blackhole	0	0

Keys

Collection of complex pattern recognition and threat string algorithms designed to remove recipient-based, intra-domain recipients employed by that domain for use as spam traps.

DNE Elements Description	Active Domains (Quaran)	Active Recip (Quaran)
Heuris. Recip Numeric Complex Pattern	0	0
Heuristic DomainKey	2	2
Heuristic RecipientKey	165	173
Heuristic RecipientKey Complex Pattern	0	0
Heuristic RecipientKey Pattern	5	11

Network Protected (advanced)

Typically, this outsourced managed spam and virus security SaaS (software as a service) used as a perimeter or front-end external firewall between you and the domain of the email address. This service uses extensive anti-spam filters and sophisticated virus scanning algorithms to stop spam and viruses before the email is to be forwarded along to actual intended recipient email address.

Network Protected Domains, and the recipients belonging to, are considered to be deliverable. However the managed SMTP SaaS's are known to be highly collaborative, checking and notifying other leading industry DNSBL sites in real-time if email sent to a anti-spam solution is deemed spam. This section is designed to provide NOTICE ONLY as to which domains are being managed by a particular third party, anti-spam solution and aid in the delivery of your email.

Recommend Usage: The anti-spam solution classifications shown below are specifically designed to aid in deliverability challenges. For example, if you are unable to get any email thru to any domain protected by a Barracuda appliance due to Barracuda labeling your email as spam, then using the Barracuda export provide below would provide options not normally available. The sender could elect to suppress this domain grouping completely to protect to deliverability to the remaining domains within your list. Another option would be to take all the domain grouping's shown below and send to after you have send all other data marked as safe or certified to ensure optimal delivery footprint.

SaaS Elements Description	Active Domains (Quaran)	Active Recip (Quaran)
AppRiver (010)	4	5
Barracuda (011)	20	23

SaaS Elements Description	Active Domains (Quaran)	Active Recip (Quaran)
Blocklist.de Reporting Service (039)	0	0
CatchAll (027)	0	0
Cisco Netprotect (042)	0	0
CloudMark (029)	0	0
CommTouch (028)	0	0
Google/Postini-McAfeeASAP.com (012)	0	0
Government; .gov, .mil, .edu, .us (030)	1	3
Invalument (022)	0	0
Ironport (013)	0	0
Kundenserver (035)	0	0
Microsoft Frontbridge (038)	0	0
Microsoft Message Security (bigfish,frontbridge) (037)	0	0
NAI-McAfee (014)	0	0
Outblaze (015)	0	0
ProofPoint Threat Intelligence (SORBS parent) (036)	0	0
RBLSMTPD (026)	0	0
Securence (016)	0	0
SpamCop Enabled User Network (041)	0	0
Symantec-BrightMail (017)	0	0
SymantecMail (019)	0	0
Symantec-MessageLabs (018)	2	3
Trend Micro (034)	0	0
XMission Envelope (043)	0	0
ZeroSpam.ca (025)	0	0

Engagement Propensity

Increase the value of your marketing campaigns with predictive engagement analytics. Gain actionable insight into which recipients are most likely to respond to your messaging and allow for development of more profitable relations with your target audience.

Our propensity to engage model predicts how likely it is that a customer will click on your email links. Armed with this information you can decide not to send an email to a certain “low likelihood to click” segment while providing a better eReputation or delivery environment aiding in a higher quality click or conversion ratio.

DNE Elements Description	Active Domains (Quaran)	Active Recip (Quaran)
Disposable Email Address	0	0
Non-Individual, Group or Role Account	2,959	2,984
Offensive KeyWord	1	1

Data Export Specifications

Manifest of deliverables contained within compressed file named:

Example: **Sample List.zip**

The following export files contain the full row of fields initially provided in comma-delimited or CSV files unless noted otherwise:

Export File Name	Export Count
Sample List DOMESTIC.txt	**5,275**
Sample List INTERNAT.txt	**13**
Sample List FULLROW.txt	**5,275**

WARNING: The following categories contain email addresses should not be mailed to without expecting potentially significant delivery issues and possible damage to the sender's online reputation.

Export File Name	Export Count
Sample List-DNE.txt	**3,292**

Note: This Do Not Email, or Bad, all-in-one file is designed for usage as a suppression file containing all file exports except CertDom, CertInt and NetProtect.txt

Also contained within the /DNEDetail folder contains the following individual exports, designed for custom usage.

Export File Name	Export Count
Sample List-INVALID.txt	**22**
Sample List-KEY.txt	**3,171**
Sample List-MOLE.txt	**21**
Sample List-NETPROTECT.txt	**34**
Sample List-PARKED.txt	**26**
Sample List-QUARANTINE.txt	**44**
Sample List-SEED.txt	**0**
Sample List-TRAP.txt	**8**

Note: This specific export appends to the full row of fields initially provided an additional field named NPD code.

If you opted for the optional single export with result descriptions contained therein, please see below. files contain the full row of fields initially provided plus an appended result code or optional result and NPD field(s) in a comma-delimited file:

Export File Name	Export Count
Sample List-COMBINED.txt	**8,614**

Note: The additional field named NPD code is optional and included only upon request before cleansing.

Protect your investment!

Clean data does have a shelf life and does not remain problem free forever.

Unfortunately due to the dynamic nature and usage of mole by many anti-spam organizations, data doesn't stay clean forever! Traps, moles and third party oversight seeds are not static. In addition, it is possible for a perfectly safe recipient one day can be turned into a mole the next day and vice versa. This happens every hour of every day and for a multitude of reasons.

To combat this ever changing environment, ProShark invented an Auto-ReCleaning system designed specifically to constantly scan existing client data while providing you with the same industry-leading, daily, reporting and results daily.

How does it work? Once a file has been scanned by ProShark, it gets sent to the new auto re-cleaning environment for scheduled re-cleans. Once daily, the data gets re-cleaned using the latest scans and rule-sets for each client and the new results get sent to your FTP. You will then be notified via email that a new set of results has been sent to their FTP for removal.

Interersted? If ensuring continued maximum protection to your eReputation while maintaining an enhanced deliverability of your list, please let your ProShark representative know right away.

The recognized authority in data hygiene.

General Disclaimer: *Every reasonable effort is made to locate all known traps and threat classification elements mentioned herein, yet due to the constantly changing and dynamic nature of the online environment, we can not guarantee the results or deliverable will be free of any/all traps or threat classification elements identified within this report.*

While every attempt has been made to ensure that the information in this document is accurate and complete, some typographical errors or technical inaccuracies may exist. ProShark does not accept responsibility for any kind of loss resulting from the use of information contained in this document. The information contained in this document is subject to change without notice.