IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 1:16-cv-00993 (GBL/TCB)

FILED UNDER SEAL PURSUANT TO LOCAL RULE 5

DECLARATION OF JASON L. NORTON IN SUPPORT OF MICROSOFT'S *EX PARTE* MOTION TO SUPPLEMENT PRELIMINARY INJUNCTION ORDER

I, Jason L. Norton, declare as follows:

1. I am a Principal Threat Intelligence Manager in Microsoft Corporation's Threat Intelligence Center ("MSTIC"). I make this declaration in support of Microsoft's Motion to Amend Preliminary Injunction Order. I make this declaration of my own personal knowledge or on information and belief where indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. I have been employed by Microsoft since August, 2015. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. I manage a team that researches these threats to identify new forms of malware, new infrastructure used for gaining unauthorized access to customer and enterprise networks, and new methods to compromise networks or customer accounts. I define this information as Threat Intelligence and share it within Microsoft's product groups to protect against or identify attempts by unauthorized users to gain access to customer and enterprise

information systems. Prior to joining Microsoft, from 2005 to 2015, I served as a Special Agent with the United States Air Force Office of Special Investigations as a Cyber Crime Investigator. My duties in this role included assisting criminal and counterintelligence authorities investigating cyber threats to the United States Air Force, Department of Defense, and cleared defense contractors. During my professional career I have received advanced, specialized training and extensive "on the job" experience in intelligence analysis, counterintelligence, digital forensics, and cyber-crime investigations.

3. On August 2, 2016, I submitted a declaration ("August 2nd Declaration") in support of Microsoft's Application for an *Ex Parte* Temporary Restraining Order and Order To Show Cause Re Preliminary Injunction ("TRO Application"). Dkt. No. 14. On August 26, 2016, I submitted a declaration ("August 26th Declaration") in support of Microsoft's Motion to Amend Preliminary Injunction Order. Dkt. No. 36. I incorporate those declarations here.

4. On August 5, 2016, the Court granted Microsoft's TRO Application. Based on the Court's Temporary Restraining Order, Microsoft was able to cut off communications between computers and networks compromised by the Defendants and certain Internet domains used by Defendants as a command and control infrastructure. On August 12, 2016, the Court converted the TRO into a Preliminary Injunction. On August 29, 2016, the Court granted Microsoft's Motion to Amend its Preliminary Injunction Order allowing Microsoft to redirect additional Strontium-controlled domains to Microsoft's sinkhole servers.

5. Microsoft's ongoing investigation into Strontium shows that the TRO was effective in protecting many victims targeted by Strontium. For example, since the execution of the TRO, Microsoft interrupted attacks on at least 122 victims targeted by Defendants. The 122 victims were already compromised with Strontium malware at the time that the registries redirected the Strontium command and control domains to Microsoft secure servers. Since the malware communicated with Microsoft secure servers instead of Strontium's infrastructure, Microsoft was able to prevent any further network exploitation of the victim networks by

Defendants.

6. However, Defendants continue to attempt to recover from the loss of their command and control domains by registering and activating new domains for use in Strontium's command and control infrastructure.[1] The evidence gathered further indicates that Defendants have used and are using those domains to launch fresh attacks on victim networks.

7. Further, as discussed in my earlier declarations, Defendants continue to misuse Microsoft's trademarks and brand names to make their domains seem legitimate. The Microsoft marks and brands exploited or likely to be exploited by Defendants include, but are not limited, to: "365," "Azure," "Bing," "Excel," "Exchange," "Healthvault," "Hotmail," "Live," "Microsoft," "Minecraft," "MSDN," "MSFT," "MS," "MSN," ".NET," O365," "Office," "OneDrive," "Outlook," "OWA," "Passport," "PowerPoint," "SharePoint," "Skype," "Surface," "Visio," "Win," "Windows," and "Xbox." Strontium has also "blended" Microsoft trademarks with non-Microsoft trademark terms. Using such "blending" technique, Strontium added domains such as "americanprogress-outlook.com" and "login-outlook.com" to its infrastructure. In another example of blending, msmodule***.com***" was a Strontium-controlled domain taken down during the execution of the TRO. Strontium is continuing this blending technique and is now using "msmodule***.net***" to target potential victims with malware.

8. One of the basic questions faced by Microsoft's investigators in the course of their investigation into Strontium is determining whether or not a domain misusing a Microsoft trademark is actually associated with illegal activity being conducted by the Defendants. Fortunately, such a determination can be reliably made based upon what we know about Strontium and how they operate their criminal infrastructure.

9. First, the Defendants typically use a small set of distinctive malware, and this malware can be identified and distinguished from other types of malware based on several

[1] I discuss Defendants' use of Internet domains as a command and control infrastructure to further their illegal acts in my August 2nd Declaration (Docket No. 14), paragraphs 7 to 22.

specific forensic factors. The specific types of malware known to be used by Defendants is listed in Exhibit A to this Declaration. The presence of this distinctive malware therefore serves as a reliable indicator that Defendants are involved. In other words, if the malware used in a new attack matches the distinctive malware known to have been used by the Defendants in past attacks, it indicates that the actors behind the new attack are the Defendants. Further, in the future, if new malware variants or families are used by Strontium, Strontium may be identified based on the similarity of such new malware to previously used malware and previously used modes of deploying such malware.

10. Because Strontium malware is reasonably distinctive, domains that are used to deliver the Strontium malware to targeted victims and domains that are used to communicate with Strontium malware already installed on victim networks are strongly implicated as Strontium domains. For example, phishing e-mails that deliver Strontium malware in the form of weaponized documents or other attachments may come from or contain links back to particular domains. Other phishing e-mails include links to domains that Defendants have set up in advance as websites designed to download Strontium malware to the user's computer and infect it. Once installed on a computer, Strontium malware is programmed to connect to and communicate with a particular set of domains after it successfully infects a victim network. In any of these cases, the Internet domains associated with the Strontium attack are strongly implicated as Strontium domains.

11. Second, Microsoft has identified patterns in the registration information provided by Defendants when registering the domains that they use in their illegal activities.[2] The factors considered include information required to be submitted during the domain registration process and includes information such as: "name," e-mail address, address and phone number provided by the registrant, the hosting service designated, the name servers used, and the IP address

[2] To set up a new domain, Defendants need to register the domain with a company referred to as a registrar, and certain information associated with that registration is made publicly available by the registrar or can otherwise be determined.

associated with the domain. Basic registration information associated with Domains registered by Defendants in the past, including the more recent domains registered by Defendants, is included in Exhibit A. If the registration information associated with a newly identified domain closely matches the pattern associated with domains registered by the Defendants in the past, it is a strong indicator that the Defendants are behind the registration of the new domain. Further, in the future, if new information is used by Defendants, but registration patterns are similar to previously used registration patterns, this too will permit Strontium domains to be reliably identified.

12. Third, Microsoft considers the specific tactics used during a new attack. For example, Strontium Defendants often send phishing e-mails to victims in which the e-mail purports to be a notification from Microsoft to the recipient regarding an unauthorized access to the recipients Microsoft account, and requesting that the recipient reset his or her account credentials. If the victim clicks on the embedded "Change Password" button in the phishing e-mail, the victim will be connected to a Strontium-controlled website which will attempt to induce the victim to enter his account credentials. Other tactics favored by the Strontium Defendants include particular deployments of remote code execution through browser drive-by, remote code execution through malicious attachment, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on. Where the tactics used in a new attack match the tactics observed to be favored by Strontium Defendants in past attacks, it is an indication that the Strontium Defendants are behind the new attack. Consequently, a domain can be linked to the Strontium Defendants by observing the tactics used in attacks involving that domain. Further, in the future, if the details, code and mode of execution change, but the general tactics are consistent with prior tactics of Strontium, this too will permit Strontium domains to be identified.

13. Fourth, the Strontium Defendants tend to target a particular type of victim and attempt to steal particular types of information. Therefore, Microsoft can use information about

the intended victim to help determine whether or not Defendants are involved in the new attack. For example, Strontium continues to target charities, defense related industries, Non-Government Organizations (NGOs), diplomatic institutions, political operations, and military organizations in the United States, Europe, and Asia. Where an Internet domain is associated with an attack on these particular types of targets, it is a factor that is consistent with the known activity and objectives of the Defendants. Further, in the future, if the targeted individuals or institutions are consistent with prior tactics of Strontium, this too will permit Strontium domains to be identified.

14. Fifth, the Strontium Defendants have used Microsoft trademarked brands or slight misspellings of those brands (e.g., "wind0ws.kz" and "windous.kz") in the names of the domains that they register for their illegal activity. Defendants use this "blending" technique to disguise the illegal nature of their conduct from the intended target. For example, since the Court's Amended Preliminary Injunction Order, Strontium utilized "microsoftstoreservice.com" and "login-outlook.com" to spread malware and compromise private networks. Thus, use of Microsoft trademarks, brand names or slight misspellings or confusing variations of those trademarks or brand names in the domain name is an indicator that the domain is associated with Strontium. The list of known and likely trademarks, brands and variants used by Strontium is set forth at Exhibit A.

15. Microsoft considers many factors associated with a domain including those described above and listed in Exhibit A to make a balanced determination of whether or not a domain is being used by the Strontium Defendants.

16. Further, by studying the ways in which the Defendants have blended and incorporated Microsoft's brand names into the names of the domains used in Strontium, Microsoft is able to anticipate the domain names Defendants are most likely to choose in the future. By combining a variety of Microsoft brand names with other common terms used in the past by Defendants, Microsoft has generated a list of the domain names most likely to be used by

Defendants going forward and has attached a true and correct copy of that list as Appendix B to the Proposed Order, submitted with Microsoft's request for a supplemental preliminary injunction. Going forward, Microsoft believes these names are most likely to be chosen by Defendants for new Strontium domains.

17. Defendants continue to register domains to carry out attacks on Microsoft's technology and customers, in particular, using Microsoft's trademarks, brands and other deceptive means, despite the court's previous orders to cease that activity and despite the prior relief which removed previously used domains from Defendants' control. Given Defendants' apparent willingness to violate the court's orders on an ongoing basis, and the ease and speed with which Defendants can register Microsoft-related domains to continue their attacks, an ongoing process is needed to efficiently and quickly curtail such activities as soon as Defendants register domains for their attacks. Without such a process, Defendants will be able to continue their malicious and illegal activities, will continue to cause irreparable injury to Microsoft, its customers and the public. Without such a process, Defendants will not be deterred from engaging in such illegal and harmful activities. I have reviewed the process set forth in the proposed supplemental injunction order submitted with this declaration. Based on my experience and background, I conclude as a technical and practical matter that the process set forth in the proposed order would enable Microsoft and the Court to effectively and efficiently enforce the Court's prior and ongoing orders and stop the irreparable harm caused by Defendants' illegal activities on an ongoing basis.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 8th day of November, 2016.

Jason L. Norton

EXHIBIT A

EXHIBIT A TO DECLARATION OF JASON L. NORTON

I. Criteria Indicating Strontium Domains

Delivers malicious software, code, commands, exploits and/or “backdoor” functionality previously associated with Strontium, including but not limited to: Win32/Foosace, Coreshell, xtunnel, Backdoor:Win32/XAgentRat.A!dha, Gamefish, SPLM, Xagent, Chopstick, Oldbait, Eviltoss, Jhuhugit, Advstoreshell, Netui, Sourface, or similar code or functionality deployed in a manner previously associated with Strontium.	Associated with remote code execution through browser drive-by or malicious attachment, privilege escalation or sandbox escape, security feature bypass, social engineering based attack and/or bootstrapped add-on, escalation of privileges, DLL file backdoor, credential stealing functionality, SSL tunnel, and/or functionality to deliver code or functions to “air gapped” USB devices, deployed in a manner previously associated with Strontium or similar code or functionality.
Domain registration information	Use of Bitcoin DNS providers
Name servers	Start of Authority (SOA) records
Resolves to IP of past Strontium domain, command and control server or similar infrastructure	Resolves to IP used in past Strontium malware
Used to deceive, target, obtain information from, and/or communicate commands or code to recipients, persons, institutions or networks previously targeted by Strontium.	Used to deceive, target, obtain information from, and/or communicate commands or code to recipients that may possess or be able to provide sensitive information or trade secrets of persons, entities or networks related to the defense, critical infrastructure or high technology sectors, journalists, political advisors or organizations, government bodies, diplomatic institutions, and/or military forces and installations.
SSL Cert Issuer_DN	SSL Cert Subject_DN
Host	Registrar

II. Known And Likely Microsoft Trademarks and Brands Used By Strontium

While Defendants may use any Microsoft marks, brands or confusingly similar indicators, Defendants have already exploited or are likely to exploit the following: “365,” “Azure,” “Bing,” “Excel,” “Exchange,” “Healthvault,” “Hotmail,” “Live,” “Microsoft,” “Minecraft,” “MSDN,” “MSFT,” “MS,” “MSN,” “.NET,” O365,” “Office,” “OneDrive,” “Outlook,” “OWA,” “Passport,” “PowerPoint,” “SharePoint,” “Skype,” “Surface,” “Visio,” “Win,” “Windows,” and “Xbox.”

While Defendants may use any keyword, in combination with Microsoft marks, brands or confusingly similar indicators, Defendants have already been seen to frequently use the following keywords:

365
64
account
accounts
adapter
adviser
american
analytic
app
assist
auth
authenticate
authorizes
bulletin
cache
care
cares
center
centr
centre
cfg
change
check
check
checksum
click
cloud
component
config
connect
consumer
content
control
corp
corporate
corporation
crc
daily
daily
data
dc
delivery
delivery
department
depatrment
dev
docs
drivadptrwin
driver
drivers

drv
edit
edit
expo
fix
forum
general
getupdate
getupdt
global
global
help
help
host
hotfix
http
id
identification
identify
identity
info
intel
intelligence
ipv4
ipv6
link
log
login
login
mail
mailbox
manager
meeting
mfa
module
monitor
mymail
net
network
news
notification
onlihe
online
panel
passport
password
password
pc
policy
politics
press
press
privacy
privacy
product
profile
profile
progress
protect
protected
redirect
reserve
review
review
scan
search
sec
secure
securing
security
security
security
send
server
service
servicing
set
setting
settings
site
srv
statistic
status
store
store
support
support
sync
sys
system
team
technology
telecom
tellekom
test
tests
tools
tools
transfer
trust
trusted
update
updater
updates
user
verify
webmail
webmail
world

The most commonly seen algorithmically predicted combinations of marks/brands and keywords are as follows, where “A” represents a mark/brand and “B” represents a keyword:

AB
BA
A-B
B-A
ABB
AB-B
A-BB
A-B-B
BAB
BA-B
B-AB
B-A-B
BBA
BB-A
B-BA
B-B-A

III. Strontium Domains Registered By Defendants To Date

Strontium Domains Addressed In Original Temporary Restraining Order

intelintelligence.org	petkrist@myself.com Pet Kristens SPAin Madrid Madrid 6251 es
outlook-security.org	k.pavuls@yahoo.com Kristen Pavuls Not Acceptable Harju Road 56 Tallin Harjumaa 15169 ee

microsoftsecurepolicy.org	ottis.davis@openmailbox.org Ottis Davis N/A Madrid Madrid Europe 133512 es
fireeyestatistic.org	luishropson@mail.com luish N/A france paris Paris none fr
adobestatistic.org	tatsuo.lesch@openmailbox.org Tatsuo Lesch Bratislava Bratislava Bratislavskykraj 21343 sk
actblues.com	contact@privacyprotect.org Domain Admin Privacy Protection Service INC d/b/a PrivacyProtect.org C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the domain owner/operator Note - Visit PrivacyProtect.org to contact the domain owner/operator Nobby Beach Queensland QLD 4218 au
akamaitechupdate.com	guiromolly@mail.com guiro molly san jose cr
dvsservice.com	fernando2011@post.com fernando N/A Victoria Victoria Victoria none au
fastcontech.com	contact@privacyprotect.org Domain Admin Privacy Protection Service INC d/b/a PrivacyProtect.org C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the domain owner/operator Note - Visit PrivacyProtect.org to contact the domain owner/operator Nobby Beach Queensland

	QLD 4218 au
intelsupportcenter.com	fisterboks@email.com Herry N/A Sweden Kronoberg KronobergelÃ¤n 5216FE se
microsoftcorpstatistic.com	welch.ebony@openmailbox.org Welch Ebony Madrid Madrid Madrid 21451 es
microsoftdccenter.com	contact@privacyprotect.org Domain Admin Privacy Protection Service INC d/b/a PrivacyProtect.org C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the domain owner/operator Note - Visit PrivacyProtect.org to contact the domain owner/operator Nobby Beach Queensland QLD 4218 au
msmodule.com	contact@privacyprotect.org Domain Admin Privacy Protection Service INC d/b/a PrivacyProtect.org C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the domain owner/operator Note - Visit PrivacyProtect.org to contact the domain owner/operator Nobby Beach Queensland QLD 4218 au
notificationstatus.com	MEELMAN@MAIL.COM DANIEL MEELMAN HOME GULLMARSVAGEN 4,JOHANNESHOV STOCKHOLM JOHANNESHOV 121 40 se
onedrivemicrosoft.com	fredmansur@mail.com Fred Mansur Mail inc 2 E 55th St, NY 10022 New York Connecticut 22100 2200 us

rsshotmail.com	nordelivery@gmail.com MIKA HANALUINEN NORD-DELIVERY mika.hanaluinen@mail.com Helsinki Helsinki 5503 fi
securemicrosoftstatistic.com	welch.ebony@openmailbox.org Welch Ebony Madrid Madrid Madrid 21451 es
adobestatistic.com	tatsuo.lesch@openmailbox.org Tatsuo Lesch Bratislava Bratislava Bratislavskykraj 21343 sk
adobeupdatetechnology.com	best.cameron@mail.com cameron N/A melbourne melbourne Western Australia none au
akamaitechnologysupport.com	bergers3008@usa.com bergers N/A Plano Plano Texas 75074 us
inteldrv64.com	chertonaksol@mail.com Feris N/A USA Buffalo New York 14202 us
intelsupportcenter.net	fisterboks@email.com Herry N/A Sweden

	Kronoberg KronobergelÃ¤n 5216FE se

Strontium Domains Addressed In August 26, 2016 Amendment To Preliminary Injunction

ms-update.info	kelsie85@mail.com Texas Towne East Sydneeberg East Sydneeberg Limburg 12124 nl
microsofthelpcenter.info	bodeverena@chewiemail.com SEVERT KERTZMANN 669 Harber Mission Apt. 021 Bechtelarport Europe 65487-0453 my
onedrive-outlook.com	fredmansur@mail.com Fred Mansur 2 E 55th St, NY 10022 New York Connecticut 22100 2200 us
onedriveoffice365.com	quitymangel@mail.com Quity Mangel Avenue du Rond-Point 9 1006 Schweiz Lausanne Schweiz Schwyz(de) 1006 ch
ms-updates.com	sandra.rafaela@chewiemail.com Sandra Rafaela Langobardenstrasse 122 Wien Wien 1220 at
ipv6-microsoft.com	contact@privacyprotect.org C/O ID#10760, PO Box 16 Nobby Beach Queensland QLD 4218 au
winsyscheck.com	anderson.neoma@openmailbox.org Anderson Neoma Helsinki Helsinki South-West Finland 43215 fi
ms-drivadptrwin.com	mr.michoverton@mail.com michel 55 Massachusetts Ave. West Acton l London Southampton (Cityof) 6360 gb
cloudmicrosoft365.com	maxvadison@mail.com

	Max Vadison 33247 Hwy 72 Golden Hwy 33247 no
account-office365.com	Quity Mangel Avenue du Rond-Point 9 1006 Schweiz Lausanne Schweiz Schwyz(de) 1006 ch
windowsappstore.net	windowsappstore.net@domainsbyproxy.com 14747 N Northsight Blvd Suite 111, PMB 309 Scottsdale Arizona 85260 us
windowsupdater.net	burnice86@openmailbox.org Burn Ice Bucharest Bucharest Bucuresti 23451 ro
microsoftdriver.com	microsoftdriver.com@domainsbyproxy.com 14747 N Northsight Blvd Suite 111, PMB 309 Scottsdale Arizona 85260 us
changepassword-hotmail.com	whoisproxy@value-domain.com 3-1 Ofuka-cho, Grand Front Osaka Tower B 23F Kita-ku Osaka-shi Osaka 530-0011 jp
privacy-hotmail.com	whoisproxy@value-domain.com 3-1 Ofuka-cho, Grand Front Osaka Tower B 23F Kita-ku Osaka-shi Osaka 530-0011 jp
hotmail-monitor.com	whoisproxy@value-domain.com 3-1 Ofuka-cho, Grand Front Osaka Tower B 23F Kita-ku Osaka-shi Osaka 530-0011 jp
livemicrosoft.net	whoisproxy@value-domain.com 3-1 Ofuka-cho, Grand Front Osaka Tower B 23F Kita-ku Osaka-shi Osaka 530-0011 jp
microsoftonlihe.com	buil_comon@mail.com Buil Comon Germany Berlin Hessen de

New Strontium Domains As Of November 9, 2016

supports-microsoft.com	rodneybleavy@mail.com Rodney C. Leavy 2698 Central Avenue Rochelle Park, NJ 07662
updates-windows.com	rodneybleavy@mail.com Rodney C. Leavy 2698 Central Avenue Rochelle Park, NJ 07662
ms-update.net	leonelcbarrett@mail.com Leonel C. Barrett Choices 3113 Winding Way Providence, Rhode Island 02903
americanprogress-outlook.com	fusbender@tutanota.com Fus Bender Vasstun 1, 5750 Odda, Norway Odda Oppland 5750 NO
login-outlook.com	alexfcloud@tutanota.com Alex Mizel Ferdinand Bolstraat 333, 1072 LH Amsterdam Other 1072 NL
msmodule.net	martin_gr86@mail.com Martin Greeg Ferdinand Bolstraat 333 Amsterdam Noord-Holland 1072 LH NL
microsoftstoreservice.com	craft030795@mail.com craft jery calle gran largo 153 paris Eure none FR
americanprogress-office365.com	fusbender@tutanota.com Fus Bender Vasstun 1, 5750 Odda, Norway Odda Oppland 5750

	NO
office365-microsoft.com	maxvalentine@tutanota.com Max Vlentine Buch corp Revay u. 24, 1065 Budapest Budapest 1065 HU
OfficeMicroUpdate.com	contact@privacyprotect.org Domain Admin Privacy Protection Service INC d/b/a PrivacyProtect.org C/O ID#10760, PO Box 16 Note - Visit PrivacyProtect.org to contact the domain owner/operator Note - Visit PrivacyProtect.org to contact the domain owner/operator Nobby Beach Queensland QLD 4218 au
dotnetupdatechecker.com	snellemanp@yandex.com Parel Snelleman Groene weide 8 Arnhem Gelderland 6833 BB NL
msnsupportcare.com	bahadirelands@mail.com Bahadir Elands Avant Garde Interior Designs 4882 Sycamore Lake Road Appleton, WI 54911 Hispanic American Samoa 399-76 US
officeupdater.com	gremblemailon@mail.com Martin Gremble Atkinson St Regina Saskatchewan SK S4N 3W4 CA
windowsxupdate.com	ggiphil@usa.com Phil Phil Now Now Georgia 1232543 US
msofficeinstall.com	tanji52@usa.com

	Tanner Abolaji Tanner Street 6 Street Alaska 3243536 US
onedrive-office365.com	maxvalentine@tutanota.com Max Vlentine Buch corp Révay u. 24, 1065 Budapest Budapest 1065 HU
loqin-microsoftonline.com	nmike83@outlook.com Mike Nowel Lucisca st 98 p 6 Colorado Drenthe 10030 NL
account-microsoftonline.com	nmike83@outlook.com Mike Nowel MNS butter st. 21 Milkona 29 st 3 New-York CO 10030 US
microsoftsupp.com	cathiedurgan@mail.md CATH EDURGAN TOWER,3-10-10,IIDABASHI,CHIYODA-KU TOKYO CHIYODA-KU 102-8460 JP