Information protection

Frequently Asked Questions

What happened?

On January 27, 2015, we discovered that malware had been installed on some of Aurora’s workstations and servers via a sophisticated cyber attack.

Immediately upon discovery, we launched an internal investigation and engaged one of the nation’s premier cybersecurity firms to remove the malware and conduct a forensics analysis. The investigation concluded that the malware was designed to intercept active sessions and capture login information when users accessed certain websites, mostly financial in nature and some social media sites. We are also working with the FBI to gain a better understanding of who is behind this attack. That investigation is ongoing.

When did it happen?

Our team discovered the malware on January 27, 2015. Out of an abundance of caution, we’re encouraging caregivers who may have used the workstations for personal use dating back six months from the time we discovered the malware to change their login credentials to sites that contain sensitive information, such as personal financial institutions and social media sites, and take advantage of credit and identity monitoring services.

What is malware?

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

What was the purpose of the malware?

The malware was designed to intercept active sessions and capture login information when users accessed one or more of a list of approximately 100 primarily financial, banking and social media websites.
A list of the sites that we know were targets is available on our intranet. A list of those sites is also below:

180solutions.com
5min.com
access.jpmorgan.com
accessonline.abnamro.com
adworldmedia.com
amazonaws.com
api.skype.com
audatexsolutions.com
auditude.com
bankeft.com
bing.com
blilk.com
brightcove.com
businessaccess.citibank.citigroup.com
businessbankingcenter.synovus.com
business-eb.ibankingservices.com
business-eb.ibankingservices.com
businessinternetbanking.synovus.com
businessonline.huntington.com
businessonline.tdbank.com
cashproonline.bankofamerica.com
cashproonline.bankofamerica.com
cbs.firstcitizensonline.com/corpach/
chsec.wellsfargo.com
clients.mindbodyonline.com
cmol.bbt.com

emoneyger.com
eorezo.com
etsy.com
express.53.com
facebook.com
farmville.com
firstmeritib.com
fwmrm.net
gator.com
goldleafach.com
googleusercontent.com
hotbar.com
iachwellsprod.wellsfargo.com
ibc.klikbca.com
internetoptimizer.com
iris.sovereignbank.com
itreasury.regions.com
itreasurypr.regions.com
king.com
kixeye.com
ktt.key.com
loyaltyconnect.ihg.com
lphbs.com
mail.google.com
mail.services.live.com
mapquest.com

owlforce.com
paylinks.cunet.org
paylinks.cunet.org
phantomefx.com
playtoga.com
premierview.membersunited.org
premierview.membersunited.org
providentnjolb.com
r777r.info
radialpoint.com
salesforce.com
scotiaconnect.scotiabank.com
search.msn.com
securentrycorp.amegybank.com
securentrycorp.zionsbank.com
securestudies.com
seekmo.com
singlepoint.usbank.com
sipuku.com
spamblockerutility.com
storage.live.com
svbconnect.com
tbreport.bellsouth.net
tcfexpressbusiness.com
tmcb.zionsbank.com
treas-mgt.frostbank.com

commercial.bnc.ca
commercial.wachovia.com
commercial2.wachovia.com
commercial3.wachovia.com
commercial4.wachovia.com
conduitservices.com
contacts.msn.com
cpwachweb.bankofamerica.com
ctm.53.com
digitalmediacommunications.com
directline4biz.com.webcashmgmt.com
directpay.wellsfargo.com
each.bremer.com
ebankingservices.com
efacts.org
mendeley.com
messenger.live.com
microsoft.com
mochibot.com
moneymanagergps.com
mozilla.com
mozilla.org
mybrowserbar.com
myshopres.com
netconnect.bokf.com
netflix.com
newasp.com
ocm.suntrust.com
officeapps.live.com
otm.suntrust.com
treasury.pncbank.com
trz.tranzact.org
trz.tranzact.org
tssportal.jpmorgan.com
tubemogul.com
twimg.com
wc.wachovia.com
wcp.wachovia.com
web-access.com
web-cashplus.com
webexpress.tdbank.com
webhancer.com
wellsoffice.wellsfargo.com
wildtangent.com
wpzkq.com
youtube.com
zango.com
zynga.com

Would I have needed to go to these specific URLs to be affected?

No. While these are the key sites affected, variations of these URLs could have been impacted as well. Additionally, this may not be an exhaustive list.

Is my information secure?

We have no evidence to suggest that sensitive information has been misused. However, we encourage all caregivers who may have used one or more of Aurora’s workstations for personal use to change their login credentials to sites that contain sensitive information, such as their personal financial institutions and social media sites. We also advise that individuals take advantage of the free credit and identity monitoring services we are offering and to be vigilant to the possibility of fraud by reviewing their credit report and credit card, bank and other financial statements for any unauthorized activity. Enrollment information for the free credit and identity monitoring services is provided in the letter mailed to affected individuals.

Was any other personal information affected?

We have no evidence that the malware accessed any health or insurance information of caregivers or patients. Additionally, we have no evidence that the malware accessed *Smart*Chart or MyHRConnection (PeopleSoft) systems.

What is Aurora doing to prevent future incidents?
To help prevent an incident like this in the future, we have implemented additional safeguards, including the installation of upgraded audit and surveillance technologies to detect unauthorized intrusions and advanced encryption technologies to protect information assets, such as laptops that may contain sensitive information. Additionally, we are reinforcing our existing policies and processes.

Does this mean I am the victim of identity theft?

No. We have no reason to believe that sensitive information has been misused. As a precaution, however, we recommend you follow the steps included in the letter sent to you regarding the free credit and identity monitoring services.

How will I know if my information was used by someone else?

We encourage you to take advantage of the one year of free credit and identity monitoring services we are offering and to be vigilant to the possibility of fraud and identity theft by reviewing your credit report and credit card, bank, and other financial statements for any unauthorized activity. Enrollment information for the free credit and identity monitoring services is provided in the letter mailed to your home.

Is credit monitoring available for my deceased family member who worked for Aurora during this time?

Credit monitoring organizations do not offer monitoring services for deceased individuals. However, there are steps you can take. An executor or surviving spouse can place a request to any of the three credit reporting agencies for a copy of the deceased individual’s credit report and take action to protect against misuse:

- “Deceased – Do not issue credit”; or
- “If an application is made for credit, please notify the following person(s) (e.g. surviving relative, executor/trustee of the estate and/or local law enforcement agency – noting the relationship).”

Contact information for the three nationwide credit reporting companies is as follows:

Equifax
PO Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-525-6285

Experian
PO Box 9554
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
PO Box 6790
Fullerton, CA 92834
www.transunion.com
1-800-680-7289

For more information regarding identity theft and the deceased, please visit http://www.idtheftcenter.org and search for “FS 117 - Identity Theft and the Deceased - Prevention and Victim Tips.” It is recommended that you also notify the Social Security Administration and Internal Revenue Service of the death of your family member and that you received this letter.

Is credit monitoring available for caregivers who are minors?

Yes, credit and identity monitoring services are available for minors. Parents or legal guardians of affected minors are being offered the opportunity to enroll in Experian’s Family Secure product. Minor employee’s notification letters contain information on enrolling in Experian’s Family Secure product.

I am no longer a caregiver of Aurora Health Care. Why did I get this letter?

As a former caregiver, you may have used an Aurora workstation during the six-month period prior to the discovery of the malware. Out of an abundance of caution, we are encouraging all caregivers, current or former, from this time period to take advantage of free credit and identity monitoring services.

How does someone obtain a free copy of their credit report?

You may obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting companies. To order your annual free report, please visit www.annualcreditreport.com, call toll free at 1-877-322-8228, or directly contact the three nationwide credit reporting companies:

Equifax
PO Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-525-6285

Experian
PO Box 9554
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
PO Box 6790
Fullerton, CA 92834
www.transunion.com
1-800-680-7289

You will also have access to your credit report if you take advantage of the free credit and identity monitoring services we are offering. Enrollment information for the free credit and identity monitoring services is provided in the letter sent to you, as well as on Caregiver Connect.

Who can I contact for additional information?

If you have any questions or concerns, please call 1-888-593-5904, Monday through Friday, between the hours of 8 a.m. and 8 p.m. Central, or email us at InformationProtection@aurora.org.

We have also posted details regarding this matter and the ongoing investigation to Caregiver Connect.

Please note that we understand that not everyone has ready access to Caregiver Connect. We have included things like a FAQ in your package home to make obtaining information as easy as possible.