UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __33__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

From: (b)(3):6(f),(b)(4)

Sent: Monday, November 05, 2012 9:53 AM
To: Jenner Holden
Subject: Your request, <<Vulnerability Fix - Disable AutoComplete>> has been logged with request id ##81911##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 81911. The details of your request are below. The status of the request can be tracked at
(b)(3):6(f),(b)(4)

Request ID: 81911
Priority : High
Urgency :
Status : Open

Due By: Nov 6, 2012 03:52 PM
Subject : Vulnerability Fix - Disable AutoComplete.
Description : Vulnerability discovered during recent penetration test.

A number of fields that contain sensitive information in Member Portal do not have autocomplete disabled. Consequently, data from these fields may be stored by the web browser.

(b)(3):6(f),(b)(4)

Fields:
(b)(3):6(f),(b)(4)

Thanks - Jenner

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here:
Close Request

Thank you for contacting LifeLock(R) Helpdesk.

From: (b)(3):6(f),(b)(4)
Sent: Monday, November 05, 2012 9:57 AM
To: Jenner Holden
Subject: Your request, <<Vulnerability Remediation - Fix Caching Directive>> has been logged with request id ##81913##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 81913. The details of your request are below. The status of the request can be tracked at (b)(3):6(f),(b)(4)

Request ID: 81913
Priority : High
Urgency :
Status : Open

Due By: Nov 6, 2012 03:57 PM
Subject : Vulnerability Remediation - Fix Caching Directive.
Description : Vulnerability discovered during recent penetration test.

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

The penetration tester found this vulnerability on www.lifelock.com. Please validate the cache-control settings for secure.lifelock.com as well.

Thanks - Jenner

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here: Close Request

Thank you for contacting LifeLock(R) Helpdesk.

From: (b)(3):6(f),(b)(4)
Sent: Monday, November 05, 2012 10:04 AM
To: Jenner Holden
Subject: Your request, <<Vulnerability Remediation - Cookie Settings>> has been logged with request id ##81915##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 81915. The details of your request are below. The status of the request can be tracked at (b)(3):6(f),(b)(4)

Request ID: 81915
Priority : High
Urgency :
Status : Open

Due By: N/A
Subject : Vulnerability Remediation - Cookie Settings.
Description :
This vulnerability was discovered during a recent penetration test.

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

Thanks - Jenner

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here: Close Request

Thank you for contacting LifeLock(R) Helpdesk.

From: (b)(3):6(f),(b)(4)

Sent: Monday, November 05, 2012 10:16 AM
To: Jenner Holden
Subject: Your request, <<Vulnerability Remediation - HTTP Response Information Disclosure>> has been logged with request id ##81916##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 81916. The details of your request are below. The status of the request can be tracked at
(b)(3):6(f),(b)(4)

Request ID: 81916
Priority : High
Urgency :
Status : Open

Due By: Nov 6, 2012 04:16 PM
Subject : Vulnerability Remediation - HTTP Response Information Disclosure.
Description : This vulnerability was discovered during a recent penetration test.

(b)(3):6(f),(b)(4)

Thanks - Jenner

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here:
Close Request

Thank you for contacting LifeLock(R) Helpdesk.

From: (b)(3):6(f),(b)(4)
Sent: Monday, November 05, 2012 11:38 AM
To: Jenner Holden
Subject: Your request, <<Vulnerability Remediation - Hidden Directory Enumeration>> has been logged with request id ##81926##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 81926. The details of your request are below. The status of the request can be tracked at (b)(3):6(f),(b)(4)

Request ID: 81926
Priority : High
Urgency :
Status : Open

Due By: N/A
Subject : Vulnerability Remediation - Hidden Directory Enumeration.
Description :
This vulnerability was discovered during a recent penetration test.

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

Thanks - Jenner

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here: Close Request

Thank you for contacting LifeLock(R) Helpdesk.

From: (b)(3):6(f),(b)(4)

Sent: Monday, November 05, 2012 12:21 PM
To: Jenner Holden
Subject: Your request, <<Vulnerability Remediation - No Clickjacking Protection>> has been logged with request id ##81932##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 81932. The details of your request are below. The status of the request can be tracked at
(b)(3):6(f),(b)(4)

Request ID: 81932
Priority : High
Urgency :
Status : Open

Due By: N/A
Subject : Vulnerability Remediation - No Clickjacking Protection.
Description : This vulnerability was discovered during a recent penetration test.

(b)(3):6(f),(b)(4)

For more information, please see:
https://www.owasp.org/index.php/Clickjacking https://www.owasp.org/index.php/Cross_Frame_Scripting
https://developer.mozilla.org/en/The_X-Frame-Options_response_header http://en.wikipedia.org/wiki/Framekiller

Please evaluate this, as this change may impact the user experience.

Thanks - Jenner

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here:
Close Request

Thank you for contacting LifeLock(R) Helpdesk.

From: Jenner Holden [/O=LIFELOCK/OU=EXCHANGE ADMINISTRATIVE GROUP REDACTED CN=RECIPIENTS/CN=JENNER.HOLDEN]
Sent: Thursday, December 06, 2012 10:27 AM
To: (b)(3):6(f),(b)(4)
Subject: FW: Your request, <<VRR REDACTED .lifelock.ad) - Directory Traversal>> has been logged with request id ##83219##

Importance: High

FYI – I submitted a VRR for the directory traversal issue we discussed.

Jenner Holden
Director of Information Security | **LifeLock® - Relentlessly Protecting Your Identity™**
480.457.2008 Office | (b)(6),(b)(7)(C) Cell
Jenner.Holden@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

From: (b)(3):6(f),(b)(4)
Date: Thursday, December 6, 2012 11:26 AM
To: Jenner Holden <jenner.holden@lifelock.com>
Subject: Your request, <<VRR REDACTED .lifelock.ad) - Directory Traversal>> has been logged with request id ##83219##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 83219. The details of your request are below. The status of the request can be tracked at
(b)(3):6(f),(b)(4)

Request ID: 83219
Priority : High
Urgency :
Status : Open

Due By: Dec 26, 2012 11:26 AM
Subject : VRR REDACTED REDAC - Directory Traversal.
Description : **Machine Name and/or IP:**
REDACTED

Discovery Method & Date:
Network penetration test - Nov 13, 2012

Vulnerability Details (Links, CVE #'s etc):
Directory Traversal

Description & Remediation Info:
(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here: Close Request

Thank you for contacting LifeLock(R) Helpdesk.

From: (b)(3):6(f),(b)(4)
Sent: Thursday, December 06, 2012 12:55 PM
To: Jenner Holden
Subject: Your request, <<VRR (Multiple Linux) - Guessable (b) (3):6(f) Manager Credentials>> has been logged with request id ##83232##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 83232. The details of your request are below. The status of the request can be tracked at (b)(3):6(f),(b)(4)

Request ID: 83232
Priority : High
Urgency :
Status : Open

Due By: Dec 26, 2012 01:55 PM
Subject : VRR (Multiple Linux) - Guessable Tomcat Manager Credentials.
Description : **Machine Name and/or IP:**
REDAC
TED

Discovery Method & Date:
Network Penetration Test, 11-12-12

Vulnerability Details (Links, CVE #'s etc):

Description & Remediation Info:
(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here: Close Request

Thank you for contacting LifeLock(R) Helpdesk.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __34__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

From: (b)(3):6(f),(b)(4)
Sent: Tuesday, April 02, 2013 10:09 AM
To: David.Bridgman@lifelock.com; Austin.Appel@lifelock.com
Subject: [Request ID :##82271##] : Added to group Information Security Team

Requester : Jenner Holden

Category : Vulnerability Remediation Request
Urgency:
Priority: High
Subject : VRR - (b)(3):6(f),(b)(4)
Description : **Machine Name and/or IP:**
(b)(3):6(f),(b)(4)

Discovery Method & Date:
Due Diligence Pen-Test by (b)(3):6((Sept 2012)

Vulnerability Details (Links, CVE #'s etc):
SSH Port Forwarding

Description & Remediation Info:
Review the following. Let me know if this is possible to address as a standard for all Linux systems.

(b)(3):6(f),(b)(4)

Click for details : (b)(3):6(f),(b)(4)

From: (b)(3):6(f),(b)(4)

Sent: Monday, November 12, 2012 12:53 PM
To: Jenner Holden
Subject: Your request, <<VRR - Missing AV (Metranet & (b)(3):6 Servers)>> has been logged with request id ##82259##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 82259. The details of your request are below. The status of the request can be tracked at
(b)(3):6(f),(b)(4)

Request ID: 82259
Priority : High
Urgency :
Status : Open

Due By: Nov 30, 2012 01:53 PM
Subject : VRR - Missing AV (Metranet & (b)(3):6(f), Servers).
Description : **Machine Name and/or IP:**
All Metranet Windows Servers & (b)(3):6 Servers

Discovery Method & Date:
Due Diligence Pen-Test by (b)(3):6(f),(b)(4) (September 2012)

Vulnerability Details (Links, CVE #'s etc):
The tester found that the hosts did not have AV installed, or the real-time scanner was disabled.

Description & Remediation Info:
(b)(3):6(f),(b)(4)

Thanks - Jenner

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here:
Close Request

Thank you for contacting LifeLock(R) Helpdesk.

From: (b)(3):6(f),(b)(4)

Sent: Monday, November 12, 2012 1:14 PM
To: Jenner Holden
Subject: Your request, <<VRR - Metranet IIS Servers Running as Local Admin>> has been logged with request id ##82263##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 82263. The details of your request are below. The status of the request can be tracked at
(b)(3):6(f),(b)(4)

Request ID: 82263
Priority : High
Urgency :
Status : Open

Due By: Nov 30, 2012 02:13 PM
Subject : VRR - Metranet IIS Servers Running as Local Admin.
Description : **Machine Name and/or IP:**
Metranet IIS Servers, specifically:
REDACTED
[redacted]

Discovery Method & Date:
Due Diligence Pen-test (September 2012)

Vulnerability Details (Links, CVE #'s etc):
IIS Services running as Local Admin

Description & Remediation Info:
(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

Mark Griffin

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here:
Close Request

Thank you for contacting LifeLock(R) Helpdesk.

From: (b)(3):6(f),(b)(4)

Sent: Monday, November 12, 2012 2:09 PM
To: Jenner Holden
Subject: Your request, <<VRR - (b)(3):6(f),(b)(4) >> has been logged with request id ##82267##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 82267. The details of your request are below. The status of the request can be tracked at
(b)(3):6(f),(b)(4)

Request ID: 82267
Priority : High
Urgency :
Status : Open

Due By: Nov 30, 2012 03:08 PM
Subject : VRR - (b)(3):6(f),(b)(4)
Description : **Machine Name and/or IP:**
(b)(3):6(f),(b)(4)

Discovery Method & Date:
Due Diligence Pen-Test by (b)(3):6(f) (Sept 2012)

Vulnerability Details (Links, CVE #'s etc):
SSH Config - PermitRootLogin set to yes

Description & Remediation Info:
(b)(3):6(f),(b)(4)

Thanks - Jenner

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here:
Close Request

Thank you for contacting LifeLock(R) Helpdesk.

From: (b)(3):6(f),(b)(4)
Sent: Monday, November 12, 2012 2:39 PM
To: Jenner Holden
Subject: Your request, <<VRR (b)(3):6(f),(b)(4) - Telnet Accessible to Public Internet>> has been logged with request id ##82273##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 82273. The details of your request are below. The status of the request can be tracked at (b)(3):6(f),(b)(4)

Request ID: 82273
Priority : High
Urgency :
Status : Open

Due By: Nov 30, 2012 03:38 PM
Subject : VRR REDACT - Telnet Accessible to Public Internet.
Description : **Machine Name and/or IP:**
REDA

Discovery Method & Date:
Due Diligence Pen Test (Sept 2012)

Vulnerability Details (Links, CVE #'s etc):
Telnet is accessible on REDAC on ports (b)(3):6(f),(b)(4)

Description & Remediation Info:
(b)(3):6(f),(b)(4)

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here: Close Request

Thank you for contacting LifeLock(R) Helpdesk.

From: (b)(3):6(f),(b)(4)
Sent: Monday, November 12, 2012 1:01 PM
To: Jenner Holden
Subject: Your request, <<VRR - REDACT - Default Credentials>> has been logged with request id ##82261##

Dear Jenner Holden,
This is an acknowledgment mail for your request. Your request has been created with id 82261. The details of your request are below. The status of the request can be tracked at (b)(3):6(f),(b)(4)

Request ID: 82261
Priority : High
Urgency :
Status : Open

Due By: Nov 30, 2012 02:00 PM
Subject : VRR - REDACTED - Default Credentials.
Description : **Machine Name and/or IP:**
REDAC

Discovery Method & Date:
Due Diligence Pen-test (September 2012)

Vulnerability Details (Links, CVE #'s etc):
(b)(3):6 Default Credentials

Description & Remediation Info:
(b)(3):6(f),(b)(4)

1. RED AC D

6. 

A technician will assist you as soon as possible. If your issue has been resolved, please close the ticket here: Close Request

Thank you for contacting LifeLock(R) Helpdesk.

From: (b)(3):6(f),(b)(4)

Sent: Friday, November 30, 2012 8:19 AM
To: Jenner Holden
Subject: Request Id ##82269##, Title VRR - (b)(3):6(f),(b)(4) has been assigned to you

82269 :: VRR - (b)(3):6(f),(b)(4) ***- Details***

Created by: Jenner Holden
Priority: High
Due by date: Nov 30, 2012 03:17 PM
Category: Vulnerability Remediation Request

Description:
Machine Name and/or IP:
(b)(3):6(f),(b)(4)

Discovery Method & Date:
Due Diligence Pen-Test by (b)(3):6(f) (Sept 2012)

Vulnerability Details (Links, CVE #'s etc):
SUDO Config - Overly Permissive

Description & Remediation Info:
(b)(3):6(f),(b)(4)

Link to request: (b)(3):6(f),(b)(4)

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __35__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

From: (b)(3):6(f),(b)(4)

Sent: Wednesday, November 28, 2012 7:39 AM
To: Jenner Holden
Subject: Request id: ##81913## has been closed.

Dear Jenner Holden,

Request 81913 opened by you was closed.

The title of the request is : Vulnerability Remediation - Fix Caching Directive

The description is: Vulnerability discovered during recent penetration test.

(b)(3):6(f),(b)(4)

Thanks - Jenner

Resolution is : Member Portal already has "no-cache" setting enabled, and WWW should be allowed to leverage browser caching since it's a public content based website. Jenner has also agreed to close the ticket.

Complete details of the request can be viewed at
(b)(3):6(f),(b)(4)

If you are not satisfied with this resolution, reply to this mail to re-open the request.

If this issue is resolved, please do not reply as it will re-open this request.

Thank you.
LifeLock IT Support

From: (b)(3):6(f),(b)(4)
Sent: Friday, December 07, 2012 2:20 PM
To: Jenner Holden
Subject: Request id: ##82273## has been closed.

Dear Jenner Holden,

Request 82273 opened by you was closed.

The title of the request is : VRR REDACT - Telnet Accessible to Public Internet

The description is: **Machine Name and/or IP:**
REDAC

Discovery Method & Date:
Due Diligence Pen Test (Sept 2012)

Vulnerability Details (Links, CVE #'s etc):
Telnet is accessible on REDAC on ports 2002, 4002, 6002, 9002

Description & Remediation Info:
(b)(3):6(f),(b)(4)

Resolution is : Telnet is disabled on this host.

Confirmed that ports are closed to telnet connections via external server on 12/7

Complete details of the request can be viewed at (b)(3):6(f),(b)(4)

If you are not satisfied with this resolution, reply to this mail to re-open the request.

If this issue is resolved, please do not reply as it will re-open this request.

Thank you.
LifeLock IT Support

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __36__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

From: (b)(3):6(f),(b)(4)
Sent: Tuesday, July 16, 2013 11:50 AM
To: David Bridgman; AnneMarie Olson; Michael Peters
Cc: Tony Valentine
Subject: Pen Tests and Remediation Internal Conversation from (b)(3):6(f) for PCI

Importance: High

Michael, Dave and Anne-Marie,

There was a PenTest report that (b)(3):6 is utilizing for PCI (referenced below) and he has now asked "Is there proof that these items have been remediated or addressed (as accepted, deferred, etc).

Dave, you were the one here when the (b)(3):6 (f),(b)(4) Pen Test was issued, which Tony says was in January.

Michael and Anne-Marie, if these items were not addressed somehow (through a remediation plan or something like this), then what will suffice for the auditor today is a plan to address the findings in the pen test. This will not hold up the RoC. (b)(3):6(tells me that he will dance around it.

HOPEFULLY, there was some plan, even if not completely remediated. Dave? Do you know?

(b)(3):6(f),(b)(4)

From: (b)(3):6(f),(b)(4)
Sent: Monday, July 15, 2013 10:57 PM
To: David Bridgman; (b)(3):6(f),(b) ; Tony Valentine
Subject: Now that I have good pen test reports

I have a question. I've uploaded (b)(3):6(*comments on pen test reports* into the From (b)(3):6(folder in the Admin, General folder in the 2013 PCI Audit folder.

(b)(3):6(f)

From: David Bridgman [David.Bridgman@lifelock.com]
Sent: Tuesday, July 16, 2013 1:07 PM
To: (b)(3):6(f),(b)(
Subject: FW: Pen Tests and Remediation Internal Conversation from (b) for PCI
Attachments: Pen-Test Remediation.docx; Pen-Test Remediation.docx

Importance: High

David Bridgman, CISSP

Sr. Information Security Engineer | **LifeLock® - Relentlessly Protecting Your Identity™**

480.457.2029 Office | (b)(6),(b)(7)(C) Cell

David.Bridgman@lifelock.com

60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

From: (b)(3):6(f),(b)(4)
Date: Tuesday, July 16, 2013 11:50 AM
To: David Bridgman <david.bridgman@lifelock.com>, AnneMarie Olson <AnneMarie.Olson@lifelock.com>, Michael Peters <Michael.Peters@lifelock.com>
Cc: Tony Valentine <Tony.Valentine@lifelock.com>
Subject: Pen Tests and Remediation Internal Conversation from Cristy for PCI

Michael, Dave and Anne-Marie,

There was a PenTest report that (b)(3) is utilizing for PCI (referenced below) and he has now asked "Is there proof that these items have been remediated or addressed (as accepted, deferred, etc).

Dave, you were the one here when the (b)(3):6(f) Pen Test was issued, which Tony says was in January.

Michael and Anne-Marie, if these items were not addressed somehow (through a remediation plan or something like this), then what will suffice for the auditor today is a plan to address the findings in the pen test. This will not hold up the RoC. (b)(3) tells me that he will dance around it.

HOPEFULLY, there was some plan, even if not completely remediated. Dave? Do you know?

(b)(3):6(f),(b)(4)

From: (b)(3):6(f),(b)(4)
Sent: Monday, July 15, 2013 10:57 PM
To: David Bridgman; (b)(3):6(f),(b Tony Valentine
Subject: Now that I have good pen test reports

I have a question. I've uploaded (b)(3): *comments on pen test reports* into the From (b)(3):6(folder in the Admin, General folder in the 2013 PCI Audit folder.

(b)(3):6(

Information Security

LifeLock

September 2012 Penetration Test (WWW, Enrollment, & Member Portal)

Vulnerability Remediation

The penetration test performed against LifeLock (www, Enrollment, & Member Portal) by (b)(3):6(f),(b)(4) in September 2012 resulted in 12 issues, with remediation recommendations. This document outlines LifeLock's intentions regarding the 12 issues raised.

Finding	Remediation Procedure	LifeLock Intention	Remediation Details
1 – XSS on (b)(3):6(f),(b)(4)	(b)(3):6(f),(b)(4)	Accept Finding and Remediate	Fix went into production on 8-30-12
2 – Weak Password Requirements		Accept Finding and Remediate	False Positive – confirmed by InfoSec that member portal requires 7 characters, one number, one capital, and one symbol
3 – Autocomplete not disabled		Accept Finding and Remediate	(b)(3):6(f), # 81911 (on-hold for system stability projects)
4 – Sensitive Data Displayed		Accept Finding and Remediate	PM (Michele Grant) has added masking of DL#, and Bank #, to product enhancement queue.
5 – Improper caching directive		Accept Finding and Remediate	(b)(3):6(f), # 81913 Completed 11-28-12
6 – insecure cookie		Accept Finding and Remediate	(b)(3):6(f), # 81915 (on-hold for system stability projects)
7 – Cookie path not set		Accept Finding and Remediate	(b)(3):6(f), # 81915 (on-hold for system stability projects)
8 – Cookie not HTTP only		Accept Finding and Remediate	(b)(3):6(f), # 81915 (on-hold for system stability projects)
9 – HTTP Response disclosure		Accept Finding and Remediate	(b)(3):6(f), # 81916 (on-hold for system stability projects)
10 – Directory enumeration		Accept Finding and Remediate	(b)(3):6(f), # 81926 (on-hold for system stability projects)

	(b)(3):6(f),(b)(4)		
11 No Clickjacking Protection		Accept Finding and Remediate	(b)(3):6(f), # 81932 (on-hold for system stability projects)
12 – Robots.txt		Accept Finding and Remediate	Evaluate contents of robot.txt file. Contents evaluated by InfoSec on 11-12-12. No issues found, no remediation is necessary.

Information Security

LifeLock

November 2012 Network Penetration Test (b)(3):6(f), (b)(4)

Vulnerability Remediation

The penetration test performed against LifeLock by (b)(3):6 in November 2012 resulted in 14 issues, with remediation recommendations. This document outlines LifeLock's intentions regarding the 14 issues raised.

Finding	Remediation Procedure	LifeLock Intention	Remediation Details
Perimeter Network Test			
1 – SSL Weak Ciphers	(b)(3):6(f),(b)(4)	Validate Issue & Remediate	Cert for REDACTE is adequate (risk accepted) REDACTE D is old ticket #83627.
2 – Autocomplete Web Forms		Validate Issue & Remediate	Accept risk for REDACTE (b)(3):6(f), (b)(4) #81911 (on-hold for system stability projects)
		Network Test	
1 – Directory Traversal		Validate Issue & Remediate	(b)(3):6(f),(#83219
2 – Local Admin Password Reuse		Validate Issue & Remediate	(b)(3):6(f), #83228
3 – Guessable Password		Validate Issue & Remediate	(b)(3):6(f), #83232
4 – Tomcat Version		Validate Issue & Remediate	False positive – internal scanning (w/ credentials) finds no issues with tomcat version.
5 – Apache Version		Validate Issue & Remediate	(b)(3):6(f), #81592 (In progress before assessment)
6 – Information Disclosure		Validate Issue & Remediate	(b)(3):6(f), (b)(4) #83629
7 – SMB Null Sessions		Validate Issue & Remediate	Risk Accepted

LifeLock

8 – Subversion Information Disclosure	(b)(3):6(f),(b)(4)	Validate Issue & Remediate	(b)(3):6(f), (b)(4) #83631 (completed)
9 – SMB Signing		Validate Issue & Remediate	Risk Accepted (Windows is evaluating the possibility of making this change)
10 – Telnet		Validate Issue & Remediate	Risk Accepted – These are VIPs. Covered by our internal scans of the "real" instance.
11 – MS12-070 Patch		Validate Issue & Remediate	False positive – internal scanning (w/ credentials) does not find this issue with SQL Server
12 – SSL Cert Issues		Validate Issue & Remediate	These interfaces are not for production data use (mostly admin consoles only) – Risk Accepted
13 – SNMP Default String		Validate Issue & Remediate	(b)(3):6(f), (b)(4) #81253 #81254 #81256 #81262
14 – RDP Issues		Validate Issue & Remediate	Risk Accepted (Windows is evaluating the possibility of making this change)

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __37__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

From: (b)(3):6(f),(b)(4)
Sent: Tuesday, July 16, 2013 2:40 PM
To: (b)(3):6(f),(b)(4) Brian Kao
Cc: Connie Suoo; Tony Valentine; (b)(3):6(f),(b)(4)
Subject: RE: Urgent Request: PCI Evidence Gathering -- (b)(3):6(f),(b)(4) Ticket 81911
Attachments: security.xlsx

Please find the attached xls with all of the security requests that I have on my backlog (initiated by Jenner).

From: (b)(3):6(f),(b)(4)
Sent: Tuesday, July 16, 2013 2:29 PM
To: (b)(3):6(f),(b) ; Brian Kao
Cc: Connie Suoo; Tony Valentine; (b)(3):6(f),(b)(4)
Subject: RE: Urgent Request: PCI Evidence Gathering -- (b)(3):6(f),(b) Ticket 81911

(b)
(3):6(f

Just to be clear, I just need the screenshot. If these items have not been remediated to-date, that is a different concern that will be addressed (probably initiated form Tony).

The priority is today, if at all possible, because the Auditor wants the remediation effort evidence before signing off on the RoC (report of compliance), and our previous PCI compliance certification is expired, and our Processor (Litle) is requesting our new RoC.

Again, I do apologize for the urgency of the request. This request just came to me about a half hour ago.

(b)(3):6(f),(b)(4)

From: (b)(3):6(f),(b)(4)
Sent: Tuesday, July 16, 2013 2:17 PM
To: Brian Kao; (b)(3):6(f),(b)
Cc: Connie Suoo; Tony Valentine; (b)(3):6(f),(b)(4)
Subject: RE: Urgent Request: PCI Evidence Gathering -- (b)(3):6(f),(b) Ticket 81911

(b)(3):6
IF you can help me understand the impact, I can prioritize accordingly against the other items on Support Engineering backlog.
THansk

From: Brian Kao
Sent: Tuesday, July 16, 2013 1:59 PM
To: (b)(3):6(f),(b)(4)
Cc: Connie Suoo; Tony Valentine; (b)(3):6(f),(b)(4)
Subject: Re: Urgent Request: PCI Evidence Gathering -- (b)(3):6(f),(b) Ticket 81911
Importance: High

(b)
(3):6(f)

The (b) ticket is still in the (b) Backlog waiting to be prioritized (b)(3):6(f),(b)(4) Please let me know if you need additional information.

Support Engineering / SEP-288

Vulnerability Fix - Disable AutoComplete

Edit Assign Comment More Actions Start Progress Resolve Issue Workflow

Details

Type:	Story
Priority:	Critical
Affects Version/s:	None
Component/s:	Security
Labels:	None

Description

Vulnerability discovered during recent penetration test.

A number of fields that contain sensitive information in Member Portal do not have autocomplete disabled. Consequently

For each of the fields listed below, please add the AutoComplete="off" attribute. This will keep the browser from caching

Fields:
User ID on the Reset Password page
Challenge Questions in the Reset Password process
User ID in the Locked User Account Reset process
Username field on the Employee Login page on lifelock.jobs

Thanks,

Brian

From: (b)(3):6(f),(b)(4)
Date: Tuesday, July 16, 2013 1:48 PM
To: Brian Kao <brian.kao@lifelock.com>
Cc: (b)(3):6(f),(b)(4) Connie Suoo <Connie.Suoo@lifelock.com>, Tony Valentine <Tony.Valentine@lifelock.com>
Subject: Urgent Request: PCI Evidence Gathering -- (b)(3):6(f),(b)(4) Ticket 81911

Hi Brian,

I am getting to the end of the PCI audit, and the Auditor wants evidence of remediation efforts (whether done or not) for a Pen Test (b)(3):6(f),(b)(4) performed last year.

This ticket 81911 (in (b)(3):6(f),(b)(4) and was assigned to you) references that it has been transferred to a (b)(3): ticket.

Can you please send me a screenshot of where the ticket is in progress? I will need this for the (b)(3):6(f),(b)(4) and preferably today.

I am truly sorry about the impromptu quick request. He is here just finishing up and if we are completed today he will sign the RoC today.

I may have other requests coming if the remediation was moved to (b)(3):6 I am going ticket by ticket to get to the (b)(3):6(f),(b)(4)

Thank you!

(b)(3):6(f),(b)(4)

FTC has submitted ‘Ex. 37 - Lifelock-0025175 (REDACTED).xlsx’ in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __38__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

From: AnneMarie Olson [AnneMarie.Olson@lifelock.com]
Sent: Friday, October 11, 2013 11:16 AM
To: Michele Grant; (b)(3):6(f),(
Cc: (b)(3):6(f),(b) AnneMarie Olson
Subject: Security Vulnerabilities

Okay, I know what these are now. These are vulnerabilities that were identified in assessments completed in September and November 2012 and should have been remediated months ago. Unfortunately, the tickets were closed when they were moved to (b)(so we didn't know.....because they have been sitting in backlog for all this time, I am going to complete risk assessments on the vulnerabilities and then speak with the business to discuss remediation.

(b) let's talk next week. I'd like to understand how we can ensure these don't slip through the crack again (other than our tracking the vulnerability fixes, which I'm going to discuss with (b) . amo

From: AnneMarie Olson
Sent: Friday, October 11, 2013 10:30 AM
To: Michele Grant
Cc: (b)(3):6(f),(
Subject: RE: Moving stories to the correct backlog

Michele,
I'm even more concerned to know these are already in production. Who can I work with to discuss these vulnerabilities further? I'd like to complete a risk assessment so that the business can decide how soon they need to be fixed. amo

From: anne-marie olson (b)(3):6(f),(b)(4)
Sent: Thursday, October 10, 2013 1:03 PM
To: AnneMarie Olson
Subject: Fwd: Moving stories to the correct backlog

---------- Forwarded message ----------
From: **Michele Grant** <Michele.Grant@lifelock.com>
Date: Thu, Oct 10, 2013 at 11:00 AM
Subject: RE: Moving stories to the correct backlog

To: anne-marie olson <(b)(6),(b)(7)(C)>, (b)(3):6(f),(b)(4)
Cc: "annemarie.olson@lifelock.com" <annemarie.olson@lifelock.com>

Sorry Anne-Marie, they were listed at the bottom of the email. Here they are:

- EAD-61 Vulnerability Fix - Disable AutoComplete (Vulnerability issues related to Member Portal)
- EAD-63 Vulnerability Remediation - Cookie Settings (Potential hijack situation with Member Portal)
- EAD-64 Vulnerability Remediation - HTTP Response Information Disclosure
- EAD-62 Vulnerability Remediation - No Clickjacking Protection (Vulnerability issues related to Member Portal)

Please let me know if these came from you. I'm fairly certain these pertain to code that is already in production rather than code waiting to go to production.

Michele

Michele Grant

Senior Product Manager | **LifeLock® - Relentlessly Protecting Your Identity™**

949.788.0607 x6022 Office | (b)(6),(b)(7)(C) Cell

michele.grant@lifelock.com

20 Pacifica, Suite 300, Irvine, CA 92618

From: anne-marie olson [mailto:(b)(6),(b)(7)(C)
Sent: Wednesday, October 09, 2013 12:50 PM
To: (b)(3):6(f),

Cc: Michele Grant; annemarie.olson@ifelock.com
Subject: Re: Moving stories to the correct backlog

Generally, security vulnerabilities should be remediated prior to going to production. Not sure if that helps because I don't know what the vulnerabilities are. Glad to discuss further if you need. amo

On Mon, Oct 7, 2013 at 6:27 PM, Erik Heyeck (b)(3):6(f),(b)(4) wrote:

Michele,

(b)(3):6 might know the answers you are looking for. These stories were created under her supervision. I have not met with Info Security to get their input into these stories.

I would suggest reaching out at AMO (Annemarie) and getting security's prioritization.

Sorry I couldn't help more.

(b)(3):6(f)

Sent from my iPhone

On Oct 7, 2013, at 1:15 PM, "Michele Grant" <Michele.Grant@lifelock.com> wrote:

(b)(3):6(f)

The ones you have marked for Retention look like high priority security issues to me. Is that right? What is the expected timeline for completion? My concern is that the Retention team is already committed to high priorities for the rest of the year and we may not have capacity. I may need to fight for an additional resource. I'm wondering if these are critical enough to help me do that.

Thank you,

Michele

Michele Grant

Senior Product Manager | **LifeLock® - Relentlessly Protecting Your Identity™**

949.788.0607 x6022 Office | (b)(6),(b)(7)(C) Cell

michele.grant@lifelock.com

20 Pacifica, Suite 300, Irvine, CA 92618

From: Farrah Holman
Sent: Monday, October 07, 2013 11:32 AM
To: Michele Grant
Subject: FW: Moving stories to the correct backlog

Michele,

Can you take a look at the stories below for Retention and move the stories into Retention if you agree?

Thanks,

Farrah Holman, PMP

Program Manager | **LifeLock® - Relentlessly Protecting Your Identity™**

480.457.5127 Office | (b)(6),(b)(7)(C) Cell

farrah.holman@lifelock.com

60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

From: (b)(3):6(f),(b)(4)
Sent: Monday, October 07, 2013 9:01 AM
To: (b)(3):6(f),(b)(4) Farrah Holman
Subject: RE: Moving stories to the correct backlog

Thank (b)(3):6(

For the vulnerability ones, those should be prioritized ahead…

(b)(3):6

From: (b)(3):6(f),
Sent: Friday, October 04, 2013 4:01 PM
To: (b)(3):6(f),(b)(4) Farrah Holman
Cc:
Subject: Moving stories to the correct backlog

All,

I'm have been going thru my Enterprise backlog and I believe the following user stories are in my backlog in error. I do not want to move them to your project's without you knowing. Please review these tasks with your PO and if you agree they belong in your backlog please feel free to take them. Please let me know which ones you do not take so I can properly plan a roadmap. The language in ( ) parentheses is my findings on these stories. The language before the () is from the user story. Thanks, (b)(3):6

(b)(3):6(f),(b)(4)

- EAD-66 MetraNet Account Reconciler Job shall provision PENDING accounts in Billing system (According to (b)(3):6(f),(b) the core team is taking care of this story)

- EAD-86 IVR Batch Job - Date difference error. (Alert phone calls are failing due to daylight savings time. The re-factored code no longer ignores this situation. Members are not getting their alert phone call)

- EAD-112 Analyze Enrollment throughput and identify the bottlenecks (The ticket does not describe which system is impacted, only that 25 concurrent enrollments are allowed at one time)

- EAD-104 Annual renewal notices going to monthly members

- EAD-134 IDV report / incident auto (this is a fulfillment error. Enterprise does partner batch jobs, not fulfillment batch jobs)

(b)(3):6(f),(b)(4)

- EAD-60 Vulnerability Remediation - Hidden Directory Enumeration (potential hijacking situation. It's unclear which site the ticket is referring to with this finding, please check www.lifelock.com, secure.lifelock.com, and lifelock.jobs.)

- EAD-95 Vulnerability Remediation - Reflected XSS (Vulnerability issues related to Webstore)

Farrah – B2B

- EAD-120 Motivano job writing PII to log files (This is an impact to the B2B file processing process)

Farrah – Retention

- EAD-61 Vulnerability Fix - Disable AutoComplete (Vulnerability issues related to (b)(3):6(f),(b)(4)
- EAD-63 Vulnerability Remediation - Cookie Settings (Potential hijack situation with (b)(3):6(f),(b)
- EAD-64 Vulnerability Remediation - HTTP Response Information Disclosure
- EAD-62 Vulnerability Remediation - No Clickjacking Protection (Vulnerability issues related to (b)(3):6(f),(b)(4)
- EAD-111 (Service Session ID) As LifeLock, I will collect data to run reports, so that I can determine how our service teams are performing across internal and external sources and across all platforms. (This is a modification/integration between (b)(3):6 phone vendor and (b)(3):6(f),(b) It is to ass the phone session ID on service call)

Thanks,

(b)(3):6

(b)(3):6(f),(b)(4)

The information contained in this transmission may contain privileged and confidential information. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __39__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

From: Austin Appel [Austin.Appel@lifelock.com]
Sent: Tuesday, November 05, 2013 3:51 PM
To: (b)(3):6(f),(b)(4)
Subject: Outstanding Penetration Test issues

Color legend:
Tickets we don't know status on – to ask scrummasters
Tickets that are waiting on us
Tickets waiting on other teams

September 2012 (b)(3):6 Partners Due Dilligence)

- 2 Secure & HttpOnly Flags for cookies on secure.lifelock.com – (b)(3) # 81915
- 4a – Version disclosed for (b)(3):6(f), (b)(4) # 81916
- 4b – Version disclosed for # 81916
- 4c – Version disclosed for Apache – (b)(3):6(f) 81916
- 4d – Version disclosed for Tomcat – (b)(3):6(f) 81916
- 7 – Reflected XSS – (b)(81953
- 9 – Missing AV – (b)(83359 – Our action – was assigned to (b)(3):6(f) for acceptance – (b)(3):6(f),(b)(4) (b)(3):6(f),(
- 12 – Web service accounts with local admin – (b)(3) 82263 – Our action – was assigned to (b)(3):6(f) for acceptance – (b)(3):6(f),(b)(4)
- 13 – Local Administrator Accounts – (b)(3) 83228 – Our action – Assigned to me for verification of remediation action
- 14 – SSH Service Permits Root Logon – (b)(3) 82267 – Our action – I was waiting on (b)(3):6(f) to output me a report using Tripwire to respond to (b)(3):6 comment of "Default configs should be used by all systems which has this off by default, please provide us a report of ones that do not if you find them," so this could be fixed.
- 15 – SUDO overly permissive – (b)(3) 82269 – Our action – was assigned to (b)(3):6(f) for acceptance – (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4)
- 18 – SSH Port Forwarding – (b)(3):6 82271 – Our action – was assigned to (b)(3):6(f) for acceptance – (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(
- 31 – Outdated version of Axway (Tumbleweed) – (b)(3) NONE – Linux team has been in the process of doing this upgrade since I got here – was there ever a ticket for this?

November 2012 (b)(3):6 (f),(b)(4)

- 1 – SSL Weak Ciphers – (b)(3) 83627 – device has apparently been waiting to be turned off since April 10th – Check with network to verify if this has been done
- 2 – Autocomplete Web Forms – (b)(3) 81911
- 1- Directory traversal – (b)(3) 83219 – Our action – Assigned to me for verification of remediation action
- 2- Guessable Password – (b)(3) 83232 – Our action – Assigned to me for verification of remediation action
- 5 – Apache Version – (b)(81592 – Last action was on Jul 30th by Windows team saying that apache update is still a release candidate – Our action – ask them the status of this and if it is still not released, defer
- 6 – Information disclosure – (b)(3 83629 – Our action - Assigned to me for verification of remediation action
- 13 – SNMP default string – (b)(3) 81253, 81254, 81256, 81262 Our action - Assigned to me for verification of remediation action

September 2012 (www, enrollment, member portal)

- 3 – Autocomplete not disabled – (b)(3) 81911 – also reported above
- 6 – Insecure cookie – (b)(3) 81915 – also reported above

- 7 – Cookie path not set – (b) 81915 – also reported above
- 8 – Cookie not HTTP only – (b) 81915 – also reported above
- 9 – HTTP response disclosure – (b) 81916 – also reported above
- 10 – directory enumeration – (b)(81926
- 11 – No clickjacking protection – (b) 81932

Austin Appel
Information Security Analyst I **LifeLock® - Relentlessly Protecting Your Identity™**
O: 480.457.2061 | M: (b)(6),(b)(7)(C)
Austin.Appel@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __40__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Exhibit also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

CONFIDENTIAL

Greenberg Traurig

Andrew G. Berg
Tel 202.331.3181
Fax 202.331.3101
berga@gtlaw.com

September 19, 2014

Gregory Madden, Esq.
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mailcode: CC-9528
Washington, DC 20580

Re: LifeLock, Inc.

Dear Mr. Madden:

This responds to your letter dated September 2, 2014 in which you made follow-up inquires to our previous submissions relating to LifeLock's information and data security practices. We have set forth the requested information (subject to your modification to those requests by e-mail dated September 11, 2014) following the order of the requests in your letter. (Please note that your questions are set forth below in bold typeface).

Response to Penetration Test Findings

Included in the documents that were provided to the FTC were "Vulnerability Remediation Requests" ("VRR") related to findings resulting from third party penetration tests of LifeLock's systems. Each of these VRRs was given a ticket number.

1) **For each of the VRR ticket numbers identified below, please describe how the request was addressed.**

VRR 81911 - See Bates Number LIFELOCK-0089185
VRR 81915 - See Bates Number LIFELOCK-0089212
VRR 81916 - See Bates Number LIFELOCK-0089214
VRR 81926 - See Bates Number LIFELOCK-0089223
VRR 81932 - See Bates Number LIFELOCK-0089225
VRR 81953 - See Bates Number LIFELOCK-0089227
VRR 82259 - See Bates Number LIFELOCK-0089258
VRR 82261 - See Bates Number LIFELOCK-0089259
VRR 82263 - See Bates Number LIFELOCK-0089261
VRR 82267 - See Bates Number LIFELOCK-0089263
VRR 82269 - See Bates Number LIFELOCK-0089330
VRR 82271 - See Bates Number LIFELOCK-0037592
VRR 83219 - See Bates Number LIFELOCK-0089117

Include in your description what steps were taken to address each VRR, identify the date each such step was taken, identify the individuals involved in each step, and identify the status of the request at this time.

The referenced VRR tickets were all opened in late 2012 and handled by the former Information Security group within their (b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

The chart below provides the requested details for each of the referenced VRR tickets.

VRR No.	Description	Steps to Address/Date	Participants	Status
81911	Disable Auto Complete	○ The vulnerability was placed into the Software Engineers' ticket system, in the backlog for the scrum team for further review. Nov '12 ○ The ticket was closed by the Scrum Master without documentation of evaluation. Aug '14 ○ The Information Security Engineering team re-evaluated the vulnerability and determined that the vulnerability cannot be controlled within the application settings. It is controlled by the user's browser. Sep '14	Information Security Software Engineering PMO	Closed
81915	Cookie Settings	○ The vulnerability was placed into the Software Engineers' ticket system, in the backlog for the scrum team for further review. Nov '12 ○ The ticket was closed by the Scrum Master without documentation of evaluation. Aug '14 ○ The Information Security Engineering team re-evaluated the vulnerability and it has been re-submitted to the Software Engineering team for remediation. Sep '14	Information Security Software Engineering PMO	Re-Opened
81916	HTTP Response	○ The vulnerability was placed into the Software Engineers' ticket system, in the backlog for the scrum team for further review. Nov '12 ○ The ticket was closed by the Scrum Master without documentation of evaluation. Aug '14 ○ The Information Security Engineering team re-evaluated the vulnerability and it has been re-assigned to the Network team for remediation. Sep '14	Information Security Software Engineering PMO	Re-Opened and Reassigned to Network
81926	Hidden Directory Enumeration	○ The vulnerability was placed into the Software Engineers' ticket system, in the backlog for the scrum team for further review. Nov '12 ○ The vulnerability was remediated although the ticket was not updated with a date of fix. ○ Sr. AppSec Engineer validated remediation. Jun '14	Information Security Software Engineering	Closed
81932	Click Jacking	○ The vulnerability was placed into the Software Engineers' ticket system, in the backlog for the scrum team for further review. Nov '12 ○ The ticket was closed by the Scrum Master without documentation of evaluation. Aug '14 ○ The Information Security Engineering team re-evaluated the vulnerability and determined that while the vulnerability is a low risk, it should be re-evaluated by the Sr. Application Security Engineer and the Software Engineering team for remediation or to request a risk acceptance. Sep '14	Information Security Software Engineering PMO	Re-Opened
81953	Reflected XSS	○ The vulnerability was placed into the Software Engineers' ticket system, in the backlog for the scrum team for further review. Nov '12 ○ The vulnerability was remediated although the ticket was not	Information Security Software Engineering	Closed

		updated with a date of fix. o Sr. AppSec Engineer validated remediation. Sep '14		
82259	No AntiVirus on Metranet	o The vulnerability was placed into the ticketing system for the Systems team for further review. Nov '12 o Because the system had troubles running with AV installed, the System Engineer requested an exception. Mar '13 o Because of the instability of the system and because the system was going to be replaced, the Sr. InfoSec Engineer noted that he would grant exception. Mar '13	Information Security Systems Team	Closed
82261	Validate Credentials	o A request was placed into the ticketing system for the Database Administration team for further review. The recommendation was for the DBA to review user accounts, validate that none are using default credentials, and to remove or disable accounts that are not needed. Nov '12 o Out of 20 IDs that were reviewed, one ID was determined that it was not needed and it was removed. All other accounts are needed and none are using default credentials. Mar '13	Database Administration Information Security	Closed
82263	IIS Running as Local Admin	o The vulnerability was placed into the ticketing system for the Systems team for further review. Nov '12 o The Systems Engineer was validating with Vendor that application needed IIS to run as local admin. Mar '13 o Although it is not updated about the Vendor application requirements, the System Engineer made a request for an exception. Because of the instability of the system and because the system was going to be replaced, the Sr. InfoSec Engineer noted that he would grant the exception. Mar '13	Information Security Systems Team	Closed
82267	SSH Allows Root Login	o The vulnerability was placed into the ticketing system for the Systems team for further review. Nov '12 o The Systems team remediated and validated that Server build had this disabled. Feb '13	Systems Team Information Security	Closed
82269	SUDO Config Overly Permissive	o The vulnerability was placed into the ticketing system for the Systems team for further review. Nov '12 o A regular user is requested for a password. An administrator is not. An exception was requested. o The System Engineer made a request for an exception. The compensating controls are that SUDO is already restricted only to administrators and that Tripwire would be used to monitor. The Sr. InfoSec Engineer noted that he would grant the exception. Mar '13	Systems Team Information Security	Closed
82271	SSH Port Forwarding	o The vulnerability was placed into the ticketing system for the Systems team for further review. Nov '12 o The Systems team remediated and validated that Server build had this disabled. Apr '13	Systems Team Information Security	Closed
83219	Directory Traversal Flaw	o The vulnerability was placed into the ticketing system for the Systems team for further review. Nov '12Validated by Information Security Engineering that it is no longer an issue. Sep '14	Systems Team Information Security	Closed

2) **Please produce the documents identified in the Comments section for Testing Procedure 11.3.b that is located at Bates Numbers LIFELOCK-1321-22 of the Table titled "PCI Report on Compliance for LifeLock." (See highlighted portion of Attachment A hereto.) If you believe these documents have previously been produced, please identify them by Bates Number.**

The requested documents are being produced along with this response.

Monitoring Activities

1) **Please identify when the "Monitoring Procedure" was first implemented.**

Identify, by date, each instance when the monitoring procedure was not followed for:

- **Automated Alerts;**
- **Daily Reports;**
- **Weekly Reports; and**
- **Monthly Reports**

2)

a. **Identify each date that LifeLock received** (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) **referenced in Attachment B. Describe the actions that LifeLock took with respect to each such alert and include in your response the date when LifeLock took such actions with respect to each such alert. Produce all documents supporting your response. If you believe these documents have previously been produced, please identify them by Bates Number.**

b. **Identify each date that LifeLock received** (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) **referenced in Attachment B. Produce all documents supporting your response. If you believe these documents have previously been produced, please identify them by Bates Number.**

c. **Identify each date that LifeLock received** (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) (b)(3):6(f),(b)(4) **reports referenced in Attachment B. Produce all documents supporting your response. If you believe these**

- (b)(3):6(f),(b)(4) is a service that provides information of what vulnerabilities could be present in an environment. The prior Information Security team chose not to implement this service.
- This service was not completely implemented to scan the LifeLock environment that the prior Information Security team was testing. As a result, the reports created by the tool are not indicative of what vulnerabilities were present.
- In lieu of (b)(3):6(f),(b)(4) LifeLock performs vulnerability scans using its (b)(3):6(f),(b)(4) and has a process to track and handle the resulting vulnerabilities. LifeLock is providing the (b)(3):6(f), (b)(4) scans for the FTC's review.

VLAN Scans

1) **Please identify all of the Virtual Local Area Networks (VLANs) referenced in (b)(3):6(f),(b)(4) statement that "not all PCI vlans were being scanned." See Bates Number LIFELOCK-0031169, July 15, 2013 email from (b)(3):6(f),(b)(4) (b)(3):6(f), to Tony Valentine, (Attachment C hereto). Provide the dates that scans of such VLANs were conducted from October 2012 through March 2014. Produce all documents supporting your response. If you believe these documents have previously been produced, please identify them by Bates Number.**

During PCI readiness activities in 2013 (b)(3):6(f),(b)(4) became aware that there were two vLANs that were not being scanned for vulnerabilities and needed to be scanned to meet PCI requirements. Promptly upon discovery, (b)(3):6 had Austin Appel add these vLANs into the vulnerability scanning tool, (b)(3):6(f), to be scanned for the remainder of the PCI reporting period.

The VLANs are: Voice **REDACTED**, 4th St Voice **REDACTED**, and Legacy Application Network **REDACTED** They were added to (b)(3):6(f), (b)(4) on 4/4/2013 and have been scanned since then on a quarterly basis. Screenshots have been provided of the scans.

Also, since (b)(3):6(f),(b)(4) has been in the CISO position, she has worked with her team to expand vulnerability scanning to critical production vLANs, regardless if it is a PCI requirement.

Please accord the foregoing information and enclosed materials confidential treatment under the Commission's Rules of Practice.

Very truly yours,

Andrew G. Berg
Counsel to LifeLock, Inc.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __41A__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

FTC has submitted 'Ex. 41A - LIFELOCK-0138077-78 (REDACTED).xlsx' in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __41B__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

FTC has submitted 'Ex. 41B - LIFELOCK-0138077-78 (REDACTED).xlsx' in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __42__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

Security Exception
Risk Assessment Form

RAF # **001**

Vulnerability or Exception Information					
Submitter Name Title	David Bridgman Sr. Security Engineer	Manager Name Title	Rich Stebbins CIO	Date:	3/21/2013
Host Name(s)	REDACTED (b)(3):6(f), (b)(4)	IP Address(es)	REDACTED	Impact Area(s)	Billing

Description of the Vulnerability or Exception

Describe the vulnerability or exception to security policy/standards. Include as much detail to expedite the assessment of the associated risk(s).

During the PCI readiness, it was discovered that anti-virus is not installed or running on the Metranet servers.

Business Reason for Vulnerability or Exception	Describe Remediation Plan
Antivirus causes Metranet application to crash. It causes enrollments to fail due to performance problems. We tried to disable all scanning and there still seemed to be some scanning happening and we had to remove the client completely.	Replace with new product in 2014

Risk Assessment

Information Security policy mandates that all Lifelock systems run anti-virus software which monitors for, detects, and deters malicious activity. Without anti-virus software, the system is exposed to viruses which could expose Lifelock's information. The Metranet server, if exposed would give the perpetrator access to billing information that includes PII.

Describe Mitigating Controls	Risk Level
(b)(3):6(f),(b)(4)	LOW

Security Advisory Group
Risk Discussion and Acceptance

The Security Department will present the risk(s) in this RAF to the Security Advisory Group when it meets. Because this group meets monthly, RAF forms completed between meetings will be routed to the SAG for acceptance or an adhoc SAG meeting will be called. Use this section to document persons involved in the discussion and the acceptance of the risk.

Acceptor:	(b)(3):6(f),(b)(4) Director, Infrastructure	Date:	4/18/2013
Acceptor:	Security Advisory Group (SAG)	Date:	

☐Karen McGee ☒Timothy Dzierzek ☒Rich Stebbins ☒Connie Suoo ☒Tony Valentine
☒(b)(3):6(f),(b)(4) ☒(b)(3):6(f),(b)(4) ☒Natalie Dopp ☒(b)(3):6(f),(b)(4) ☒(b)(3):6(f),(b)(4)

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __43__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

From: (b)(3):6(f),(b)(4) [Stephanus.Setiawan@lifelock.com]
Sent: Wednesday, April 17, 2013 2:36 PM
To: AnneMarie Olson
Subject: Re: (b)(3):6 Lack of Antivirus on Metranet Server(s)

Accepted. Thanks

From: AnneMarie Olson <AnneMarie.Olson@lifelock.com>
Date: Wednesday, April 17, 2013 2:21 PM
To: (b)(3):6(f),(b)(4)
Cc: AnneMarie Olson <AnneMarie.Olson@lifelock.com>
Subject: FW: (b)(3): Lack of Antivirus on Metranet Server(s)

(b)(3):6(f), Have you had a chance to look at this? I need your acceptance ASAP so I can forward to the Security Advisory Group for their approval. This is an artifact for the PCI audit. amo

From: AnneMarie Olson
Sent: Monday, April 15, 2013 12:12 PM
To: (b)(3):6(f),(b)(4)
Subject: (b)(3):6 Lack of Antivirus on Metranet Server(s)

(b)(3):6(f), (
We (Security) are implementing a revised process for risk management where, among other things, we will have a person or persons accept the risk of a non-compliant security policy. This process was reviewed and agreed upon by the Security Advisory Group (SAG) which also agreed that certain other parties who, to some degree, control the risk would also accept the risk.

Such is the case with the attached (b)(3):6(f),(b)(4) which documents the fact that we do not have antivirus running on the Metranet Servers. Please review the (b) and reply to this email with "I accept this risk." I will then send to all members of the SAG for their acceptance.

If you would like to discuss, feel free to ring or stop by. amo

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __45__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document.**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __46__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

From: Gwen Ceylon
Sent: Tuesday, January 22, 2013 1:54 PM
To: Jim Shoemaker; Andrew Ureta
Cc: David Bridgman; Tony Valentine; (b)(3):6(f),(b)
Subject: Here's all your Documents and Findings on Your Systems for You to Review/Update and Remediate
Attachments: REDACTED Security Config Guide for Border Routers v4.0 (on SP).doc; RED Security Config Guide for Firewalls v6.0.docx; REDACTED Security Config Guide for Internal Routers v4.0 (on SP).doc; REDACTED Change Control Procedure v3.0 (old - on SP).doc; PCI Environment Full Vulnerability Report January Scan.xlsx; Pre-PCI 2013 Remediation Task List.xlsx; Network Open VRRs 012112.xls; (b)(3):6(f),(b Firewall PCI Check - Firemon.pdf; REDA (b)(3):6 Audit Report 20121227.pdf; REDA (b)(3):6 Audit Report 20121227.pdf; REDACTED (b)(3):6 Audit Report 20121227.pdf; REDACTED (b) Audit Report 20121227.pdf; REDACTED (b)(3):6 Audit Report 201212127.pdf

Gwen Ceylon, CISSP CISM CISA
Contractor - Information Security/Compliance
480.457.2101 Office | (b)(6),(b)(7)(C) Cell
gwen.ceylon@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281
LifeLock® - Relentlessly Protecting Your Identity™

FTC has submitted 'Ex. 46 - Lifelock-0085281_REDACTED.xlsx' in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __47__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document.**

From: Gwen Ceylon
Sent: Thursday, January 17, 2013 6:23 PM
To: Tony Valentine
Subject: FW: PCI Environment Full Vulnerability CSV Report January Scan.xlsx
Attachments: PCI Environment Full Vulnerability CSV Report January Scan.xlsx

FYI...

Gwen

From: Gwen Ceylon
Sent: Thursday, January 17, 2013 7:20 PM
To: (b)(3):6(f),(b)(4)
Subject: PCI Environment Full Vulnerability CSV Report January Scan.xlsx

(b)(3):6(f),(b)(4)

I thought I would share with you a different way to look at vulnerabilities on the systems. It's the how I like to look at it anyway.

Currently there are about 200 VRRs in (b)(3):6(f), – 136 are past due. Now some might say 200 VRRs – 200 vulnerabilities, that's not so bad. But that's not the reality. Currently there are 4669 vulnerabilities on the systems in the PCI environment. Most of them ranked critical.

Yes, looking at the first tab , those very tall World Trade Center looking bars in the red – are a bad thing.

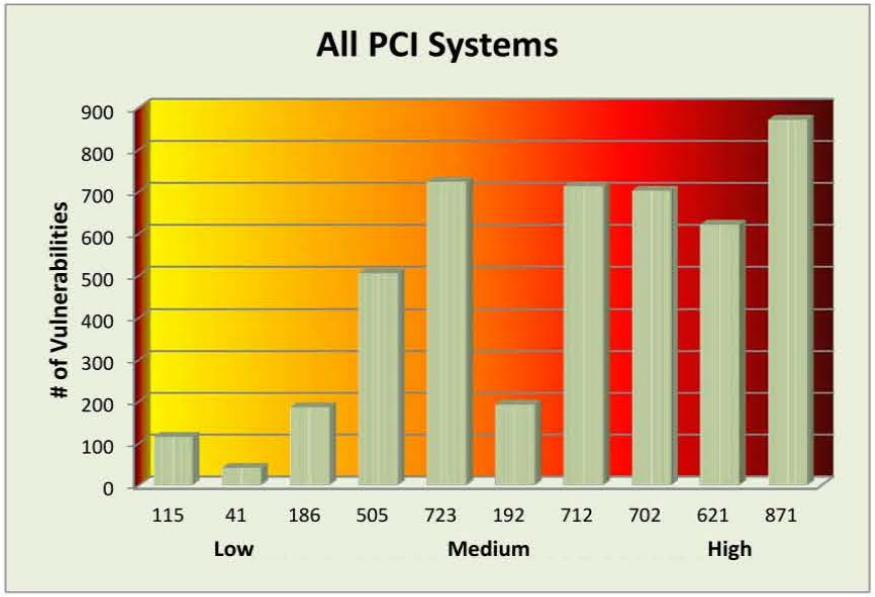
Some of the VRRs the security guys enter contain hundreds of vulnerabilities in them. Plus they set the priority of the ticket to low – making everyone believe even more it's not such a big deal. But the auditor is not going to like seeing this many critical vulnerabilities especially since control 6.2 of the PCI DSS is now a requirement that you remediate critical vulnerabilities within a month.

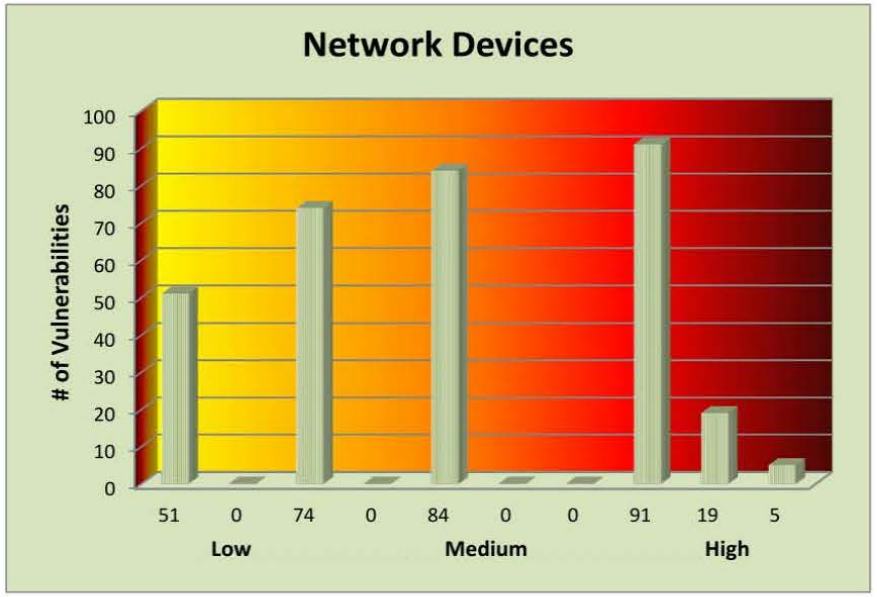
I don't know what your guys think when they open a VRR and see 100s of vulnerabilities listed by title, with maybe a CVE number or MS bulletin number with a note from Information Security saying "Please apply the patch". It's got to be overwhelming. Your guys don't have time to google ever CVE number to figure out what patch needs to be applied. This spreadsheet contains that information in the remediation column.

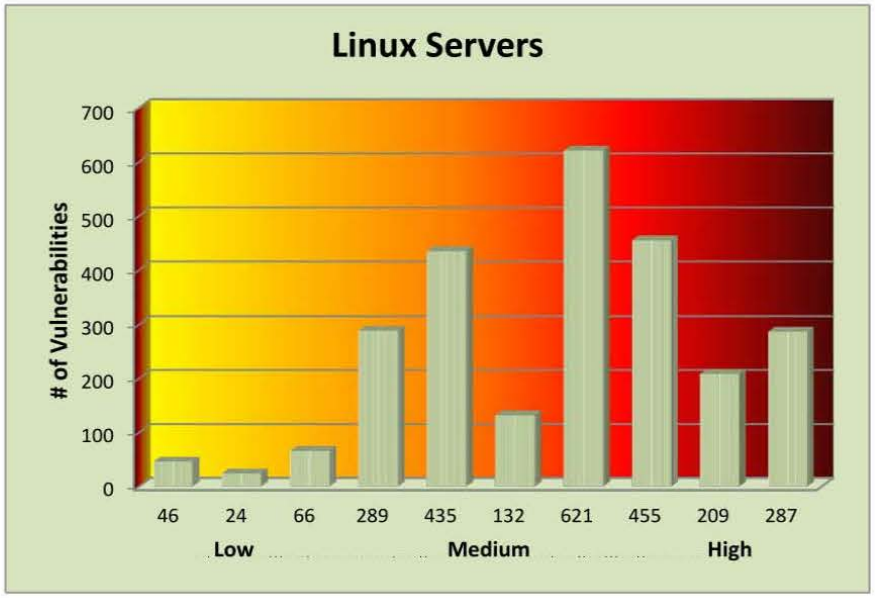
You may now be thinking, "OMG, how did we create this nightmare for ourselves?" But wait, it's not as bad as you think. 2593 of the 4669 vulnerabilities exist on just 9 systems. Get those 9 off the network, fix them, replace them, pull the plug, whatever, and over half the vulnerabilities disappear. That is a huge leap in the right direction. A different way to tackle this, but I think it is an effective way.

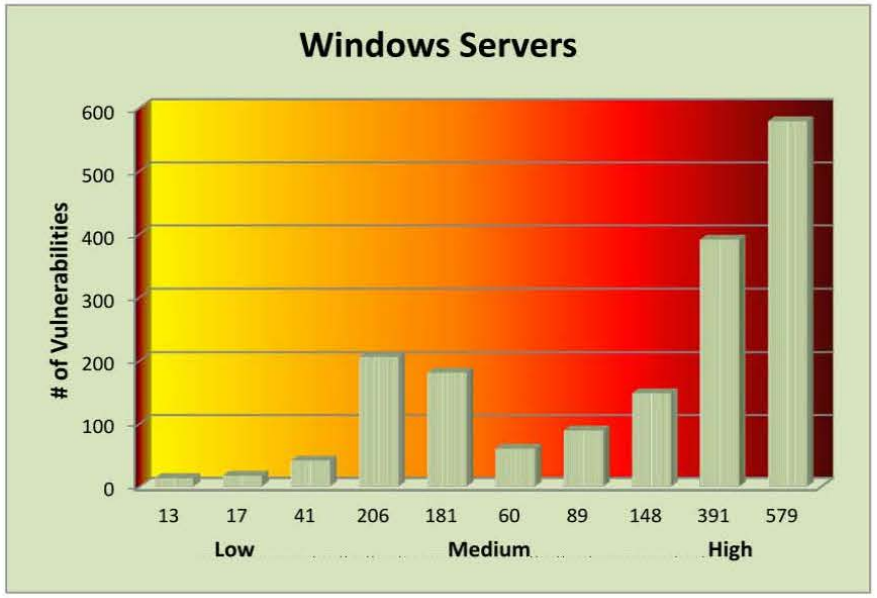
Gwen

Gwen Ceylon, CISSP CISM CISA
Contractor - Information Security/Compliance
480.457.2101 Office (b)(6),(b)(7)(C) Cell
gwen.ceylon@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281
LifeLock® - Relentlessly Protecting Your Identity™


All PCI Systems
of Vulnerabilities
900
800
700
600
500
400
300
200
100
0
115 41 186 505 723 192 712 702 621 871
Low
Medium
High


Network Devices
of Vulnerabilities
100
90
80
70
60
50
40
30
20
10
0
51 0 74 0 84 0 0 91 19 5
Low
Medium
High


Linux Servers
of Vulnerabilities
700
600
500
400
300
200
100
0
46 24 66 289 435 132 621 455 209 287
Low
Medium
High


Windows Servers
of Vulnerabilities
600
500
400
300
200
100
0
13 17 41 206 181 60 89 148 391 579
Low
Medium
High

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __48__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

From: Karen Overton [Karen.Overton@lifelock.com]
Sent: Friday, March 22, 2013 2:03 PM
To: (b)(3):6(f),(b)(4)
Cc: David Bridgman; AnneMarie Olson
Subject: Updated SOPs
Attachments: (b) Zip Procedure_update.docx.doc; Rogue Wireless Monitoring_update.docx.doc; Vulnerability Management Procedure _updated.docx.doc; Software Evaluation and Approval Procedure_update.docx.doc

Hi,

I have updated the SOPs from earlier in the week due to the "new" template. You will notice that I highlighted the areas that still need input.

Let me know if you have any questions.

Thanks for your patience during this process.

Karen Overton
Technical Writer | **LifeLock® - Relentlessly Protecting Your Identity™**
480.457.2087 Office
Karen.Overton@LifeLock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

LifeLock	Vulnerability Management Procedure	
	Content Owner:	Approved By:
Classification: Confidential	Version #: 1.0	Approval Date:
Reference No.*	ADMINISTRATION NOTES	Effective Date:

Vulnerability Management Procedure

BACKGROUND/PURPOSE

This procedure provides guidance on vulnerability management practices to identify vulnerabilities on LifeLock information systems for remediation.

Internal vulnerability scans are scans that search for misconfigured systems or systems that need updating on our network. Currently, LifeLock utilizes the (b)(3):6(f),(b)(4) and WhiteHat products for this purpose. Once a vulnerability is found, we must review it, make action decisions, and follow through on those action decisions.

PROCEDURE

Unless noted, the Information Security Team performs the following tasks.

1. Run an internal scan. Internal vulnerability scans are run periodically throughout the year:
   - Internal – (b)(3):6(f), (b)(4) every six weeks
   - External – (b)(3):6 (f),(b)(4) monthly, submitted each quarter
   - WebApp – WhiteHat: daily

   When a scan finishes, it becomes available for viewing in the respective home pages.
2. Formulate a list of actions to be done per host, using a tracking spreadsheet made from exported scan data and placed in the share drive.
   a. A search of (b)(3):6(f),(b)(4) is performed to distinguish which vulnerabilities are awaiting verification.
      - Existing tickets are marked on the tracking spreadsheet as to be closed (remediated), to be sent back
      - If a ticket exists that is still undergoing remediation efforts, it is captured in the next step (2b).
   b. Vulnerabilities are looked at host-by-host to determine new vulnerabilities.
   c. Exceptions exist for a number of previously-seen vulnerabilities. To deal with vulnerabilities from non-exempted systems:
      1. Ensure the new vulnerability matches previously seen vulnerabilities (i.e., User name is the same for a user's directory having broad permissions).
      2. Submit exemption request for new vulnerability.
      3. Information Security Team Manager reviews the exemption request and makes an action decision.
3. Work through the spreadsheet (Information Security Team) and perform the required actions:
   a. Send any existing tickets marked as "to be remediated" that show up in a new scan back to the relevant remediation group. As needed, Information Security will provide input to help the remediation team resolve the issue.

b. For previously seen vulnerabilities, adapt a duplicated previous ticket for this instance.
c. For updates, assign the following severity levels. Note that at the Information Security Team's discretion, these severity levels may vary.
    - A severity code of Medium to any updates with published Metraploit modules, exploit code, or exploit kits abusing the vulnerability.
    - A severity code of High to updates that are externally accessible.
    - A severity of Low for updates not covered above.
d. Close the relevant tickets for verified remediations.
e. Hold a meeting where each new vulnerability is discussed with its context in order to arrive at an action decision. The action decision is then executed.

4. Perform the directed remediation actions, following these SLAs for each ticket:
    - Critical priority: 48 hours
    - High priority: 2 weeks
    - Medium priority: 4 weeks
    - Low priority: 8 weeks
5. Assign the VRR (Remediation Team) back to the Information Security Team. The next vulnerability scan will run after 60 days. The vulnerability ticket will either be closed or sent back to the relevant remediation team depending on if the remediation effort was detected as being successful:

APPLICABILITY

This procedure applies to all devices in the PCI environment scope capable of propagating malicious code that are attached to the LifeLock network.

REFERENCES

What materials or documents (including other Policies, Procedures or Guidelines) are referenced in the Policy or are necessary to interpret or implement it?

CONTACT

General Questions

Questions related to this Procedure can be sent to Information Security.

REVISION HISTORY

Ver. No.	Release Date	Prepared By	Reviewed By	Approved By	Description
1.0					New Procedure
					Revision
					Annual Update

*Reference Number should be based on a three letter dept. abbreviation (FIN, LEG, P&T, MSV, HRD), an clear abbreviation of the Policy title and the Effective Date separated by underscores, e.g. "HRD_Harassment_010112".

END

LifeLock	Software Evaluation and Approval Procedure	
	Content Owner: Security Analyst IV	Approved By: Sr. Security Engineer
Classification: Confidential	Version #: 1.0	Approval Date: 03/18/13
Reference No. REDACTED	ADMINISTRATION NOTES	Effective Date: 03/18/13

Software Evaluation and Approval Procedure

BACKGROUND/PURPOSE

This procedure establishes instructions for the Information Security (IS) to manage requests from users to install new (not previously approved) software on his or her workstation or on any device managed by ATS. ***Approval of software is a joint effort between IS and UTS; both areas must approve all software.***

DEFINITIONS

SECURITY-APPROVED SOFTWARE LIST: List of software currently installed on workstations that is approved by Information Security.

PROCEDURE

User Technology Services (UTS) and Information Security (IS) must review and approve all software prior to its installation. This approval may occur on behalf of the entire organization, a subset of the organization, or at an individual level. The following outlines the steps to be taken when a user requests new software or when unapproved software is discovered on a user's workstation.

1.0 Software Requested Prior to Installation

#	Step Name	Responsibility	Relevant Functional and/or Technical Procedures
Input	Requester submits a service request ticket using (b)(3):6(f),(b) requesting installation of software.		
1.1.	Approve the software – UTS	UTS	• Using Application Management Procedure, approve the software • If not approved, notify the user via the (b)(3):6(f),(b)(4) ticket • If approved, continue to step 1.2
1.2.	Check the Security-Approved Software List to determine if software is already approved.	UTS	• If the software requested appears on the list (exactly, including version number), and conditions are met as outlined in the User Technology Software Installation Procedures, the UTS representative will install the software. • If the software requested does not appear on the list, reassign the ticket to Information Security or create a task within the ticket and assign to IS requesting an evaluation. If applicable,
1.3.	Evaluate the software	InfoSEC	• Check the developer's reputation if possible • Confirm the download site is safe (via Urlvoid, Norton Safeweb, McAfee Site Advisor, and WoT)

#	Step Name	Responsibility	Relevant Functional and/or Technical Procedures
			• Check Secunia for any known vulnerabilities. • Do a general google search for any undisclosed vulnerabilities • Upload the file to (b)(3):6(f), (b)(4) and confirm it has a safe rating • Scan the file with (b)(3):6(f),(b)(4) and confirm it comes back clean *Note that Security does not test the software for compatibility issues with the standard image or confirm the software is appropriate for the job duties of the requestor*
1.4.	Approve the software	InfoSEC	• Add the software to the Security-Approved Software List • Notify UTS they may install the software
1.5.	Do not approve the software	InfoSEC	• Notify UTS the software is not approved for installation.
1.6.	Notify User	UTS	• Notify user that either the software is installed or will be installed and continue to step 1.6 • Notify user that the software is not approved by Information Security - COMPLETE
1.7.	Install the software	UTS	COMPLETE

2.0 Unnaproved Software Discovered on Workstation

#	Step Name	Responsibility	Relevant Functional and/or Technical Procedures
Input	During workstation scan, unapproved software is discover on user's workstation	InfoSEC	• Contact the user to request the business need for the software. Remind the user they are not to download software using their admin rights. • Open an incident. • If the user provides business need for the software, continue to Step 2. • If the user is unable to provide a business need or reports he no longer needs the software, request he remove the software immediately. Rescan the workstation to validate it is removed and then update and close the incident
2.1.	Evaluate the software	InfoSEC	Use the same process as detailed in 1.2
2.2.	Approve the software	InfoSEC	• Add the software to the Security-Approved Software List. • Notify the user the software is approved and remind them again that policy prohibits them from downloading software. • Update and close the incident - COMPLETE
2.3.	Do not approve the software	InfoSEC	• Notify user that software is NOT approved and therefore he must remove the software immediately. • Rescan the workstation to validate it is removed

#	Step Name	Responsibility	Relevant Functional and/or Technical Procedures
			• Update and close the incident - COMPLETE

APPLICABILITY

All software, including freeware, COTS, et al. to be installed on a workstation. Software on servers is out of scope; in plan for Q2-2013. This procedure does not include UTS's role in software management. The Software Evaluation and Approval Procedure assumes UTS has approved the software from a functionality and management perspective as it relates to packaging, deployment, and administration. UTS maintains a separate procedure for this purpose.

REFERENCES

The following is a list of documents that support this Procedure.

- Security-Approved Software List (InfoSEC sends to UTS each month and immediately when changed)
- Application Management Procedures (UTS)

CONTACT

General Questions

Questions related to this Procedure can be sent to Information Security

REVISION HISTORY

Ver. No.	Release Date	Prepared By	Reviewed By	Approved By	Description
1.0	3/18/13	Anne-Marie Olsen/Security Analyst IV	Tim Oliver/UTS	Dave Bridgman/ Sr Security Engineer	New Procedure. Replaced Document Number [redacted] with Reference Number.
					Revision
					Annual Update

END

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __49__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

From: Austin Appel [Austin.Appel@lifelock.com]
Sent: Friday, January 03, 2014 3:13 PM
To: Mike Wan; (b)(3):6(f), (b)(4) Brian Kao
Subject: RE: Web-based vulnerabilities

Definitely. I think we already have the problem of a number of vulnerabilities in the backlog.

So we are in agreement that this is the way to go ahead and handle these tickets in the future? If so, I will start creating tickets next week following this procedure. (b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

If you ever have any questions regarding this, feel free to reach out to me at any time.

Thanks for your help!

Austin Appel
Information Security Analyst | **LifeLock® - Relentlessly Protecting Your Identity™**
O: 480.457.2061 | M: (b)(6),(b)(7)(C
Austin.Appel@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

From: Mike Wan
Sent: Friday, January 03, 2014 4:07 PM
To: (b)(3):6(f),(b Austin Appel; Brian Kao
Subject: Re: Web-based vulnerabilities

(b)(3):6(f),(b)(4)

Mike

From: (b)(3):6(f),(b)(4)
Date: Friday, January 3, 2014 2:23 PM
To: Austin Appel <Austin.Appel@lifelock.com>, Brian Kao <Brian.Kao@lifelock.com>, Mike Wan <mike.wan@lifelock.com>
Subject: Re: Web-based vulnerabilities

I am good.

From: Austin Appel <Austin.Appel@lifelock.com>
Date: Friday, January 3, 2014 3:06 PM
To: Brian Kao <Brian.Kao@lifelock.com>, (b)(3):6(f),(b)(4) Mike Wan <Mike.Wan@lifelock.com>
Subject: RE: Web-based vulnerabilities

That certainly works for me. I just want to make sure to have a process that works for you guys too though.

Austin Appel
Information Security Analyst | **LifeLock® - Relentlessly Protecting Your Identity™**
O: 480.457.2061 | M: (b)(6),(b)(7)(C)
Austin.Appel@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

From: Brian Kao
Sent: Friday, January 03, 2014 3:00 PM
To: Austin Appel; (b)(3):6(f),(b Mike Wan
Subject: Re: Web-based vulnerabilities

I think you can just assign to P&T Engineering Group, then any one of us can help converting the VRR ticket into (b)(3): What do you think (b)(3):6(f) Mike?

Brian

From: Austin Appel <Austin.Appel@lifelock.com>
Date: Friday, January 3, 2014 1:47 PM
To: (b)(3):6(f),(b)(4) Brian Kao <brian.kao@lifelock.com>, Mike Wan <Mike.Wan@lifelock.com>
Subject: Web-based vulnerabilities

We have had a number of web-based vulnerabilities in the past due to pen-tests, but we now have a dedicated web vuln scanner scanning (b)(3):6(f),(b)(4) Because of this, we may be seeing more issues to be fixed.

I know I have had some talks with a couple of you regarding the handling of these vulnerabilities, but we do need to figure out a consistent method of reporting and remediating these vulnerabilities that works for both teams.

Would the following solution work for you guys?

(b)(3):6(f),(b)(4)

If not, what do you think might work? Depending on the amount of discussion on this topic, we may want to schedule a meeting to find out what will work. The key problem that I see with the above solution is working out who gets assigned the (b)(3):6(f),(b) ticket and an easy way I can (or the Intern can) distinguish which "project" the VRR should go to to be fixed.

Let me know your thoughts on this.

Thanks,

Austin Appel
Information Security Analyst | **LifeLock® - Relentlessly Protecting Your Identity™**
O: 480.457.2061 | M: (b)(6),(b)(7)(C)
Austin.Appel@lifelock.com

60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __50__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

From: Kevin Pfister <Kevin.Pfister@lifelock.com>
Sent: Friday, August 1, 2014 9:41 AM
To: (b)(3):6(f),(b)(4)
Subject: FW: Requests Over 150 Days Still Open

(b)(

I'm working on cleaning up tickets that have been open for more than 150 days. Do you know why we have all of these VRR requests still open and assigned to Security?

Thx

Kevin Pfister
Director Application Implementation and Support | **LifeLock® - Relentlessly Protecting Your Identity™**
480.457.2078 Office | (b)(6),(b) Cell
Kevin.Pfister@LifeLock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

From: (b)(6),(b)(7)(C)
Sent: Thursday, July 31, 2014 7:25 PM
To: Kevin Pfister
Subject: Requests Over 150 Days Still Open

This includes VRRs

Requests Over 150 Days Still Open

Generated by (b)(3): on : 07/31/2014 19:24
Total records : 322

Request ID	Created Time	Created By	Department	Subcategory	Subject	Group	Technician
71546	04/09/2012 16:42	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] Security Updates (low)	Information Security	Austin Appel
71611	04/10/2012 17:00	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] - Security Updates (low)	Information Security	Austin Appel
71612	04/10/2012 17:04	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] - Security Updates (low)	Information Security	Austin Appel
74153	06/01/2012 16:04	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] http basic authentication (low)	Information Security	Austin Appel
74270	06/04/2012 15:08	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] various updates and configuration issues (low)	Information Security	N/A
75810	07/06/2012 09:04	(b)(3):6(f	Finance	Incident/Problem	Some refunds performed in AP have incorrect credit card type in Metranet	Product Owner	Ryan Friel
77761	08/15/2012 15:27	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] Guest access allowed to Windows event logs (Low)	Information Security	Austin Appel
79250	09/17/2012 17:11	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] Jenkins Advisory 2012-09-17 (med)	Information Security	Austin Appel
79560	09/24/2012 12:08	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR (All Windows workstations and [b] servers) [REDACTED] - (high)	Information Security	Austin Appel
80092	10/03/2012 15:12	(b)(3):6(f)	Finance/Accounting	Incident/Problem	Refunds Approved in MN but not by [b]	Product Owner	Erik Lamb
80516	10/11/2012 10:17	Jenner Holden	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] Apache version Update	Information Security	Austin Appel
81257	10/24/2012 16:56	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] SNMP community name	Information Security	Austin Appel
81258	10/24/2012 16:57	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] SNMP community name	Information Security	Austin Appel
81259	10/24/2012 16:58	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] - SNMP community name	Information Security	Austin Appel
81260	10/24/2012 16:59	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] SNMP community name	Information Security	Austin Appel
81264	10/24/2012 17:09	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] 'rsh' Remote Shell Service Enabled (med)	Information Security	Austin Appel
81265	10/24/2012 17:10	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] 'rsh' Remote Shell Service Enabled (med)	Information Security	Austin Appel
81269	10/24/2012 17:27	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] SSH server supports SSH protocol v1 clients (low)	Information Security	Austin Appel
81270	10/24/2012 17:27	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] SSH server supports SSH protocol v1 clients (low)	Information Security	Austin Appel
81445	10/26/2012 16:55	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] OpenSSH Update (low)	Information Security	Michael Hoffman
81446	10/26/2012 16:56	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] OpenSSH Update (low)	Information Security	Austin Appel
81447	10/26/2012 17:05	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] OpenSSH Update (low)	Information Security	Austin Appel
81448	10/26/2012 17:06	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] OpenSSH Update (low)	Information Security	Austin Appel
81450	10/26/2012 17:09	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] OpenSSH Update (low)	Information Security	Austin Appel
81470	10/26/2012 17:39	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] OpenSSH Update (low)	Information Security	Austin Appel
81471	10/26/2012 17:41	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] OpenSSH Update (low)	Information Security	Austin Appel
81473	10/26/2012 17:45	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [REDACTED] OpenSSH Update (low)	Information Security	Austin Appel
81474	10/26/2012	Austin Appel	Products & Technology	Vulnerability Remediation	VRR [REDACTED] OpenSSH	Information Security	Austin Appel

	17:46			Requests	Update (low)		
81475	10/26/2012 17:48	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] OpenSSH Update (low)	Information Security	Austin Appel
81476	10/26/2012 17:49	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] OpenSSH Update (low)	Information Security	Austin Appel
81529	10/29/2012 09:39	Jenner Holden	Products & Technology	Vulnerability Remediation Requests	VRR (partners.lifelock.com - [redacted] Browsable directory	Information Security	Austin Appel
81614	10/29/2012 16:12	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Adobe Flash permissive crossdomain.xml policy (low)	Information Security	Michael Hoffman
81915	11/05/2012 11:03	Jenner Holden	Products & Technology	Member Portal (myLL)	Vulnerability Remediation - Cookie Settings	Information Security	(b)(3):6 (f),(b)(4
82259	11/12/2012 13:53	Jenner Holden	Products & Technology	Vulnerability Remediation Requests	VRR - Missing AV (Metranet & MSSQL Servers)	Information Security	Austin Appel
82261	11/12/2012 14:00	Jenner Holden	Products & Technology	Vulnerability Remediation Requests	VRR - [redacted] Default Credentials	Information Security	Austin Appel
82263	11/12/2012 14:13	Jenner Holden	Products & Technology	Vulnerability Remediation Requests	VRR - Metranet IIS Servers Running as Local Admin	Information Security	Austin Appel
82267	11/12/2012 15:08	Jenner Holden	Products & Technology	Vulnerability Remediation Requests	VRR - Prod Linux Servers (SSH Allows Root Login)	Information Security	Austin Appel
82269	11/12/2012 15:17	Jenner Holden	Products & Technology	Vulnerability Remediation Requests	VRR - Prod Linux Servers (SUDO Permissions)	Information Security	Austin Appel
82271	11/12/2012 15:26	Jenner Holden	Products & Technology	Vulnerability Remediation Requests	VRR - Prod Linux Servers (SSH Port Forwarding)	Information Security	Austin Appel
83219	12/06/2012 11:25	Jenner Holden	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Directory Traversal	[redacted]	[redacted]
83232	12/06/2012 13:55	Jenner Holden	Products & Technology	Vulnerability Remediation Requests	VRR (Multiple Linux) Guessable Tomcat Manager Credentials	Information Security	Austin Appel
83627	12/17/2012 14:38	Jenner Holden	Products & Technology	Vulnerability Remediation Requests	VRR - [redacted] - Web VPN - No Longer Needed?	Information Security	Austin Appel
83629	12/17/2012 14:52	Jenner Holden	Products & Technology	Vulnerability Remediation Requests	VRR - Check_MK - No Authentication	Information Security	Austin Appel
84380	01/08/2013 17:13	(b)(3):6(f	Infrastructure AIS	Batch Jobs (BATCH)	HPS Feedback Files	Application Production Support	(b)(3):6(f),
84684	01/15/2013 16:09	Gwen Ceylon	Products & Technology	Vulnerability Remediation Requests	Tomcat 5.2.23 Has Multiple Vulnerabilities	Information Security	Austin Appel
85074	01/23/2013 17:02	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] WebDAV Extensions are Enabled	Information Security	Michael Hoffman
85169	01/25/2013 18:04	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR (blog.lifelock.com) - WordPress version 3.5.1	Information Security	Austin Appel
86476	02/25/2013 14:38	(b)(3):6 (f),(b)(4)	Business Operations	Metranet	Declined Refund showing as Approved in MT	Product Owner	Erik Lamb
86673	02/28/2013 10:53		Business Operations	Metranet	Declined Refund showing approved in Metranet	Product Owner	Erik Lamb
87385	03/11/2013 17:32	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates (low)	Information Security	Michael Hoffman
88334	04/01/2013 11:51	(b)(3):6(f), (b)(4)	Infrastructure AIS	Batch Jobs (BATCH)	Prosodie files being received but not marked	Application Production Support	(b)(3):6(f), (b)(4)
88349	04/01/2013 14:10		P & T	(b)(3):6(f),	Upgrade RN to the current release	Application Production Support	
89503	04/24/2013 16:29	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] IRDP (med)	Information Security	Michael Hoffman
89504	04/24/2013 16:30	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] IRDP (med)	Information Security	Michael Hoffman
89505	04/24/2013 16:31	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] IRDP (med)	Information Security	Michael Hoffman
90458	05/09/2013 12:36	(b)(3):6(f),(b)(4)	Products and Technology	B2B	Legacy B2B platform should also use enhanced B2B backup similar to AOL	Middleware (WebLogic) Support	Barry Ghotra
90776	05/14/2013 17:02		Business Operations	Product Configurator	Enhancement Request	Product Owner	(b)(3):6(f),
90812	05/15/2013 09:41	Shannon Smith	Strategic Partnerships	Report Request - Modification	Need Account Added to Partner Account Manager Report	Application Production Support	N/A
91562	05/30/2013 17:21	(b)(3):6	P & T	(b)(3):6(f),	Need AP code updated for new RN Incident Queue	Application Production Support	N/A
92771	06/25/2013 14:57	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Exported volume is publicly mountable (high)	Systems Engineering	N/A
92772	06/25/2013 14:57	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Exported volume is publicly mountable (low)	Systems Engineering	N/A
92944	06/27/2013 16:46	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - LDAP Anonymous Directory Access - (high)	Information Security	Austin Appel
92945	06/27/2013 16:47	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - LDAP Anonymous Directory Access - (high)	Information Security	Austin Appel
92946	06/27/2013 16:49	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - DLL Hijacking - (critical)	Information Security	Michael Hoffman
92947	06/27/2013 16:49	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - DLL Hijacking - (critical)	Information Security	Michael Hoffman
93196	07/02/2013 16:46	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates (med)	Systems Engineering	N/A
93198	07/02/2013 16:49	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates (med)	Systems Engineering	N/A
93199	07/02/2013 16:51	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Adobe Updates (med)	Information Security	Michael Hoffman
93200	07/02/2013 16:53	Tracey Kolnsberg	Member Services - Team J	(b)(3):6(f), (b)(4)	Add Member will not process	Middleware (WebLogic) Support	(b)(3):6(f),
93204	07/02/2013 16:58	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates (med)	Systems Engineering	N/A
93210	07/02/2013 17:08	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates (low)	Information Security	Michael Hoffman
93211	07/02/2013 17:10	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates (low)	Information Security	Austin Appel
93212	07/02/2013 17:12	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates (low)	Systems Engineering	N/A
93265	07/03/2013 11:21	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - SMTP unauthenticated 3rd-party mail relay - (critical)	Information Security	Michael Hoffman
93267	07/03/2013 11:22	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Plaintext credentials transmitted unencrypted - (high)	Information Security	Austin Appel
93901	07/17/2013 12:25	Jaramy Conners	Member Services	Member Portal (myLL)	Inaccurate Information for Credit Inquiry Alerts	Application Production Support	(b)(3):6(f),
94390	07/26/2013	(b)(3):6(f), (b)(4)	Finance	(b) (3):6(	Tensoft user access	Finance	N/A

94744	11:20 08/02/2013 14:14	(b)(3):6(f), (b)(4)	Finance/Accounting	Metranet	AVS Response Code Handling Change	Product Owner	Ryan Friel
96310	08/30/2013 04:47	Jacob Cyriac	P&T Engineering	Member Portal (myLL)	Not able to access Member portal - gettting error system is undergoing maintainence.please try again later.	Middleware (WebLogic) Support	N/A
96766	09/10/2013 15:31	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96767	09/10/2013 15:32	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96768	09/10/2013 15:34	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96769	09/10/2013 15:35	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96770	09/10/2013 15:35	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96771	09/10/2013 15:36	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96772	09/10/2013 15:37	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96773	09/10/2013 15:37	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96774	09/10/2013 15:38	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96775	09/10/2013 15:38	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96776	09/10/2013 15:40	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96778	09/10/2013 15:41	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96779	09/10/2013 15:43	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
96780	09/10/2013 15:44	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Windows Service Isolation Bypass [redacted] (high)	Systems Engineering	(b)(3):6(f), (b)(4)
96893	09/12/2013 11:20	(b)(3):6(f), (b)(4)	Finance/Accounting	Metranet	Plan change and billing system did not honor free days when it should have	Application Production Support	
96918	09/12/2013 15:52		Finance/Accounting	Metranet	Migrated Member Not Billed	Product Owner	Ryan Friel
96926	09/12/2013 18:56	Kathryn Worth	Human Resources	(b)(3):	Wellness Page	Corporate Communications	(b)(3):6
97065	09/16/2013 13:58	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Systems Engineering	N/A
97068	09/16/2013 14:16	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Update Rollup (high)	Information Security	Michael Hoffman
97070	09/16/2013 14:20	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Update Rollup (high)	Information Security	Michael Hoffman
97124	09/16/2013 16:21	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates - Adobe Flash (high)	Information Security	Austin Appel
97125	09/16/2013 16:23	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Austin Appel
97127	09/16/2013 16:26	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates (high)	Information Security	Michael Hoffman
97171	09/17/2013 14:03	Dennis Tebon	Enterprise Sales & Alliances	ReqLogic	Need to fill out a PO for an expense report and need access too (b)(3)	Purchasing	N/A
97180	09/17/2013 15:28	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] - Guest access allowed to Windows event logs (Low)	Information Security	Michael Hoffman
98342	10/11/2013 09:42	Andrew Citro	Products & Technology	Windows OS	(b)(3): not using SSL + Domain authentication being passed in the clear	Application Production Support	(b)(3):6 (f),(b)(4
98660	10/18/2013 11:12	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	N/A
98661	10/18/2013 11:12	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	N/A
98662	10/18/2013 11:14	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] ICMP redirection enabled (high)	Information Security	N/A
98663	10/18/2013 11:15	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] ICMP redirection enabled (high)	Information Security	N/A
98664	10/18/2013 11:16	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] World writable files (high)	Information Security	N/A
98665	10/18/2013 11:18	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR [redacted] World writable files (high)	Information Security	N/A
98681	10/18/2013 14:10	(b)(3):6(f), (b)(4)	Finance	(b)(3):6(f),	Passing of LL Response Code to ODS	Product Owner	(b)(3):6(f),(b
98926	10/24/2013 11:26		Business Operations	Database Creation	Access for IDA to LifeLock Systems	Database Support	N/A
98963	10/24/2013 17:00	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR (Dev, Stage, & QT env.) Data in quick search DB - (critical)	N/A	(b)(3):6(f),(
99167	10/30/2013 08:10	Bethanne Silvola	Business Operations	Agent Portal (AP)	Update Cancellation Reasons in Agent Portal	Product Owner	N/A
99592	11/12/2013 08:02	Jacob Cyriac	P&T Engineering	Agent Portal (AP)	When trying to login to AP in Dev01 , getting error page.	Middleware (WebLogic) Support	Rakesh Katpally
99860	11/14/2013 15:22	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR - Weak Keys (low)	Systems Engineering	N/A
99948	11/18/2013 07:29	Andy Doyle	P&T Infrastructure	Database Modificaton	Remove Hardcoded IP from PREN database	Application Production Support	(b)(3):6(f),
100371	11/26/2013 13:39	Greg Beaubrun	N/A	Metranet	Enrollment issues at (b)(3):6	Middleware (WebLogic) Support	N/A
100420	11/27/2013 09:57	Terence Wood	Business Operations - MS QM Team	Other	Box.com Access "Lifelock App customer log in"	Information Security	Austin Appel
100465	11/27/2013 15:09	AnneMarie Olson	Products & Technology	Oracle Database	E&Y Request to Run Scripts on Oracle DB Servers	N/A	Tony Valentine

100520	12/02/2013 10:14	Rajesh Elappan	P&T Service Deliver	Weblogic	Need Access to Weblogic Console	Middleware (WebLogic) Support	Rakesh Katpally
100592	12/03/2013 11:40	Melissa Chase	Member Operations	(b)(3):6(f),(b)(4)	Critical Error Occurred	Middleware (WebLogic) Support	N/A
100601	12/03/2013 12:50	Tracy Roberts	Member Services		Critical Error in AP	Middleware (WebLogic) Support	N/A
100604	12/03/2013 13:49	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR (blade controllers - see below) TPMI vulnerabilities (high)	Information Security	Michael Hoffman
100674	12/04/2013 14:37	AnneMarie Olson	Products & Technology	Linux / Red Hat	Q4 User Access Reviews - RH Linux	Resolution	N/A
100746	12/05/2013 16:59	Kalyani Patibandla	Information Technology	Add, Modify, Delete	Please Grant "Guest" access for Product configurator in Production for executing prod smoke tests.	Product Owner	(b)(3):6(f),(b)(4)
100787	12/06/2013 13:14	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Windows Service Isolation Bypass [redacted] (high)	Information Security	Michael Hoffman
100797	12/06/2013 15:32	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] - Apache HTTPD: ETag Inode Information Leakage (medium)	Information Security	Michael Hoffman
100799	12/06/2013 15:58	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] SNMP community name (medium)	Systems Engineering	N/A
100801	12/06/2013 16:13	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Apache HTTPD: ETag Inode Information Leakage (medium)	Information Security	Michael Hoffman
100832	12/09/2013 05:46	Jacob Cyriac	P&T Engineering	Run Query	Request to run the query in stage db.	Quality Assurance (P&T)	Jacob Cyriac
100871	12/09/2013 14:23	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] - Default or Guessable SNMP community names: public (medium)	Information Security	Michael Hoffman
100876	12/09/2013 14:47	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Invalid TLS/SSL certificate (low)	Information Security	Michael Hoffman
100996	12/11/2013 12:54	AnneMarie Olson	Products & Technology	Product Configurator	SOX Request: Product Configurator App Last Modified Date	Middleware (WebLogic) Support	Barry Ghotra
101024	12/11/2013 13:58	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (medium)	Information Security	Michael Hoffman
101149	12/12/2013 14:59	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] http basic authentication (medium)	Information Security	Michael Hoffman
101210	12/13/2013 10:44	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101220	12/13/2013 11:01	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101222	12/13/2013 11:08	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Adobe Flash permissive crossdomain.xml policy (medium)	Information Security	Michael Hoffman
101232	12/13/2013 11:38	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101233	12/13/2013 11:42	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101234	12/13/2013 11:43	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101235	12/13/2013 11:44	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101236	12/13/2013 11:45	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101237	12/13/2013 11:46	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101238	12/13/2013 11:47	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101239	12/13/2013 11:48	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101240	12/13/2013 11:49	(b)(3):6(f), [redacted]	PMO	Weblogic	11g/12c Upgrade DEV 3	Middleware (WebLogic) Support	N/A
101241	12/13/2013 11:50	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101244	12/13/2013 11:54	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101245	12/13/2013 11:55	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101246	12/13/2013 11:58	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101247	12/13/2013 11:59	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101248	12/13/2013 12:00	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101249	12/13/2013 12:02	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Update (high)	Information Security	Michael Hoffman
101251	12/13/2013 12:04	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101252	12/13/2013 12:08	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101253	12/13/2013 12:14	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101254	12/13/2013 12:20	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101257	12/13/2013 12:28	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] DLL Hijacking - (high)	Information Security	Michael Hoffman
101258	12/13/2013 12:29	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101259	12/13/2013 12:34	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] - DLL Hijacking - (high)	Information Security	Michael Hoffman
101261	12/13/2013 12:36	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (high)	Information Security	Michael Hoffman
101262	12/13/2013 12:39	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101263	12/13/2013 12:44	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Microsoft IIS Content Location Internal IP Address Leak (high)	Information Security	Michael Hoffman
101264	12/13/2013 12:50	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101267	12/13/2013 12:59	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Adobe Updates (critical)	Systems Engineering	N/A
101268	12/13/2013 13:03	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IRDP (medium)	Information Security	Michael Hoffman

101269	12/13/2013 13:04	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101270	12/13/2013 13:06	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
101271	12/13/2013 13:13	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Database open access (high)	Information Security	Michael Hoffman
101273	12/13/2013 13:16	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	[redacted] Database open access (high)	Middleware (WebLogic) Support	Barry Ghotra
101275	12/13/2013 13:20	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	[redacted] Database open access (high)	Middleware (WebLogic) Support	Barry Ghotra
101276	12/13/2013 13:22	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Database open access (high)	Information Security	Michael Hoffman
101283	12/13/2013 13:31	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Database open access (high)	Information Security	Michael Hoffman
101308	12/15/2013 13:37	Leighann Olds	N/A	(b)(3):6(f),(b)(4)	XML Error Issue	Middleware (WebLogic) Support	N/A
101309	12/15/2013 13:38	Leighann Olds	N/A		Enrollment Error	Middleware (WebLogic) Support	N/A
101333	12/16/2013 11:15	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] - Weak LAN Manager Hashing permitted (low)	Systems Engineering	N/A
101334	12/16/2013 11:19	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	[redacted] - NTP 'ntpd' Autokey Stack Buffer Overflow Vulnerability (low)	Systems Engineering	N/A
101337	12/16/2013 11:30	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	[redacted] SSH supports v1 clients (high)	Information Security	Michael Hoffman
101655	12/23/2013 14:58	Andrew Mora	P&T Infrastructure	Other	Migrate DEV databases to new QT instance	Database Support	(b)(3):6(f),(b)(4)
101722	12/27/2013 09:06	Binzer Moore	N/A	Member Portal (myLL)	L3 Issues	Middleware (WebLogic) Support	N/A
101747	12/27/2013 16:15	(b)(3):6	Marketing	InfoLock	affiliate 4 week report	Business Intelligence	(b)(3):6(f),(b)(4)
101767	12/30/2013 08:59	Andrew Citro	Products & Technology	LAN / WAN	(b)(3):6(f),(b)(4)	Information Security	Austin Appel
101806	12/30/2013 13:45	(b)(3):6(f)	P&T Quality Assurance	Add, Modify, Delete	Access request to Concur Account	Finance	Monique Jones
102021	01/06/2014 13:16	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR (stage-secure.lifelock.com) Information Leakage (high)	Middleware (WebLogic) Support	N/A
102022	01/06/2014 13:17	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR (stage-secure.lifelock.com) Information Leakage (high)	Middleware (WebLogic) Support	N/A
102023	01/06/2014 13:19	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR (stage-secure.lifelock.com) Predictable Resource (medium)	Middleware (WebLogic) Support	N/A
102025	01/06/2014 13:30	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR (stage-secure.lifelock.com) Insufficient Transport Layer Protection (high)	Information Security	Michael Hoffman
102029	01/06/2014 13:39	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR (stage-secure.lifelock.com) Non-HttpOnly Session Cookie (medium)	Product Owner	N/A
102031	01/06/2014 13:48	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR (stage-secure.lifelock.com) Unsecured Session Cookie (medium)	Information Security	Michael Hoffman
102084	01/07/2014 10:36	(b)(3):6(f),(b)(4)	Member Operations	Other	LifeLock.com	Product Owner	N/A
102223	01/09/2014 13:59		Infrastructure	Other	Request a Data Patching from Prod to Pre-Prod Environments	Database Support	(b)(3):6(f),(b)(4)
102235	01/09/2014 15:42		Business Services	(b)(3):6	Need access to the Lemon Companies in Great Plains and ReQlogic	Finance	N/A
102404	01/14/2014 08:36	Krystal Cunningham	Partner Operations	Batch Jobs (BATCH)	ABC file fail. Evaluation required to confirm formatting error	Product Owner	(b)(3):6(f),(b)(4)
102517	01/15/2014 15:22	Andrew Citro	Products & Technology	Member Portal (myLL)	Please create a Test Account in Production for security scanning	Member Operations	N/A
102519	01/15/2014 15:5	(b)(3):6(f),(b)(4)	Business Ops (QM)	Batch Jobs (BATCH)	USAirways Batch Code Errors	Product Owner	(b)(3):6(f),(b)(4)
102520	01/15/2014 15:5		Business Ops (QM)	Batch Jobs (BATCH)	United Batch Code Errors	Product Owner	
102521	01/15/2014 16:0		Business Ops (QM)	Batch Jobs (BATCH)	American Batch Code Errors	Product Owner	
102523	01/15/2014 16:0		Business Ops (QM)	Batch Jobs (BATCH)	Choice Batch Code Errors	Product Owner	
102524	01/15/2014 16:0		Business Ops (QM)	Batch Jobs (BATCH)	Hilton Batch Code Errors	Product Owner	
102525	01/15/2014 16:0		Business Ops (QM)	Batch Jobs (BATCH)	Sears Batch Code Errors	Product Owner	
102725	01/20/2014 15:2		Information Technology	Weblogic	Setup Weblogic Credentials in Prod for Ops Console	Middleware (WebLogic) Support	N/A
102728	01/20/2014 16:0		P&T Insfrastructure	Product Configurator	PROD Salesforce Opportunity Sync with Product Configurator	Middleware (WebLogic) Support	(b)(3):6(f),(b)
102738	01/20/2014 20:0		P&T Engineering - Irvine	Windows OS Issues	Jenkins is getting rn template related errors when trying to build EN-SP6_S branch , is there something going on with RN DEV?	Middleware (WebLogic) Support	N/A
102905	01/23/2014 12:0		Partner Operations	Product Configurator	List of all active campaigns/promo codes	Product Owner	N/A
102976	01/24/2014 10:57	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR (local windows workstations) Domain Admin Credential Use (high)	Systems Engineering	N/A
102980	01/24/2014 11:33	(b)(3)	Infrastructure Security	Laptop Computer	Equipment Request - Development System for AppSec	Information Security	(b)(3):6(f),(b)(4)
103131	01/28/2014 11:12	David O'Neill	Member Services Leadership	(b)(3):6(f),(b)(4)	Database Access Request: (Qfinity call recording)	Quality Assurance (MS)	
103244	01/30/2014 06:54	Bethanne Silvola	Business Operations		Table Update for No News is Good News Emails	Application Production Support	
103550	02/05/2014 07:37	(b)(3):6(f),(b)(4)	Member Operations		Daily Reporting	Resource Planning	John Clapper
103567	02/05/2014 10:04		Business Ops (QM)	Batch Jobs (BATCH)	Hilton Batch Job Code Update	Product Owner	(b)(3):6(f),(b)(4)
103617	02/05/2014 18:19		Business Ops (QM)	Batch Jobs (BATCH)	American Airline Batch File Code Fix	Product Owner	
103623	02/06/2014 07:19	Ashok Yadav	P&T Engineering	Jenkins	Jenkin Build is failing continuously	Product Owner	
103682	02/06/2014 17:06	(b)(3)	Business Ops (QM)	Batch Jobs (BATCH)	American File Needs Formatting	Product Owner	
103683	02/06/2014 17:06	Jasmeet Dhiman	Infrastructure	Furniture Repairs/Replacement	Chair Replacement	Human Resources	
103726	02/07/2014 14:39	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	[redacted] - World writable files exist (medium)	Information Security	Michael Hoffman

103729	02/07/2014 14:55	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
103730	02/07/2014 15:01	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Systems Engineering	(b)(3):6(f), (b)(4)
103731	02/07/2014 15:05	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
103733	02/07/2014 15:07	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
103735	02/07/2014 15:12	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
103770	02/09/2014 18:47	(b)(3):6(f),(b)(4)	Member Services - Team H	Mobile SMS	Unable to finish SMS opt in	Application Production Support	(b)(3):6(f), (b)(4)
103856	02/10/2014 17:56	Brian Kao	Information Technology	Tomcat	clean up phantom tomcat cache files on [redacted].lifelock.ad	Middleware (WebLogic) Support	N/A
103924	02/12/2014 04:30	(b)(3):6(f), (b)(4)	N/A	(b)(3):6(f),	AP having issues creating new incidents	Middleware (WebLogic) Support	N/A
103937	02/12/2014 10:18		P&T Infrastructure	Load Balancer	F5 Load Balancing for Exchange 2010	Network Support	(b)(3):6(f),(b)(4)
103962	02/12/2014 13:38		Business Ops (QM)	Batch Jobs (BATCH)	United Batch Code Update	Product Owner	
104038	02/13/2014 11:50		Finance/Accounting	Member Portal (myLL)	Memberships have not billed since 2012 and are still active.	Application Production Support	
104070	02/13/2014 16:51		Business Ops (QM)	Batch Jobs (BATCH)	US Airways Batch Code Update	Product Owner	
104118	02/14/2014 11:13	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
104125	02/14/2014 11:25	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
104126	02/14/2014 11:27	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
104128	02/14/2014 11:36	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
104131	02/14/2014 11:49	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	[redacted]	[redacted]
104133	02/14/2014 11:51	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
104135	02/14/2014 11:57	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] - World writable files exist (low)	Information Security	Michael Hoffman
104136	02/14/2014 12:01	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] World writable files exist (medium)	Information Security	Michael Hoffman
104137	02/14/2014 12:13	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] JBoss Incomplete Security Restraints (high)	Information Security	Michael Hoffman
104138	02/14/2014 12:14	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
104142	02/14/2014 12:24	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] - Unencrypted Telnet Service Available (high)	Information Security	Michael Hoffman
104145	02/14/2014 12:40	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
104148	02/14/2014 12:47	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
104156	02/14/2014 13:07	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
104159	02/14/2014 13:24	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] IP Source Routing (high)	Information Security	Michael Hoffman
104191	02/14/2014 15:23	Aimee Henshaw	PMO	Add, Modify, Delete	Need a Service Account for Jenkins	Systems Engineering	Michael Glenney
104279	02/18/2014 11:18	AnneMarie Olson	Products & Technology	Linux / Red Hat	Q1-14 Linux User Access Report	Systems Engineering	(b)(3):6(f), (b)(4)
104287	02/18/2014 11:28	AnneMarie Olson	Products & Technology	(b)(3):	Q1-14 WebLogic User Access Report	Middleware (WebLogic) Support	
104320	02/18/2014 14:29	Austin Appel	Products & Technology	Vulnerability Remediation Requests	VRR (All endpoints) Symantec Endpoint Protection Update (critical)	Information Security	Michael Hoffman
104349	02/18/2014 17:03	(b)(3):6(f), (b)(4)	Finance	InfoLock	Add SalesForce fields to InfoLock for Invoice Report	Business Intelligence	(b)(3):6(f),(b)(4)
104373	02/19/2014 09:14		Business Ops (QM)	Batch Jobs (BATCH)	US Airways Batch Code Update - Posting Code 11	Product Owner	
104424	02/19/2014 14:15	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
104425	02/19/2014 14:16	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (high)	Information Security	Michael Hoffman
104426	02/19/2014 14:16	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (medium)	Information Security	Michael Hoffman
104427	02/19/2014 14:18	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
104428	02/19/2014 14:22	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (medium)	Information Security	Michael Hoffman
104429	02/19/2014 14:24	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (high)	Information Security	Michael Hoffman
104430	02/19/2014 14:32	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (critical)	Information Security	Michael Hoffman
104433	02/19/2014 14:37	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (high)	Information Security	Michael Hoffman
104435	02/19/2014 14:42	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (medium)	Information Security	Michael Hoffman
104437	02/19/2014 14:49	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (high)	Information Security	Michael Hoffman
104440	02/19/2014 14:51	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (medium)	Information Security	Michael Hoffman
104441	02/19/2014 14:55	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (high)	Information Security	Michael Hoffman
104442	02/19/2014 14:55	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (medium)	Information Security	Michael Hoffman
104444	02/19/2014 14:58	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (high)	Information Security	Michael Hoffman
104445	02/19/2014 14:58	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (medium)	Information Security	Michael Hoffman
104446	02/19/2014 15:02	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (medium)	Information Security	Michael Hoffman
104447	02/19/2014	Michael Hoffman	Infrastructure	Vulnerability Remediation	VRR [redacted]	Information Security	Michael Hoffman

	15:02			Requests	Security Updates (high)		
104446	02/19/2014 15:04	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104449	02/19/2014 15:04	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (medium)	Information Security	Michael Hoffman
104450	02/19/2014 15:09	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (medium)	Information Security	Michael Hoffman
104451	02/19/2014 15:09	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104452	02/19/2014 15:12	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (medium)	Information Security	Michael Hoffman
104453	02/19/2014 15:12	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104454	02/19/2014 15:15	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104455	02/19/2014 15:15	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (medium)	Information Security	Michael Hoffman
104456	02/19/2014 15:19	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (critical)	Information Security	Michael Hoffman
104457	02/19/2014 15:22	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED	Information Security	Michael Hoffman
104458	02/19/2014 15:25	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104509	02/20/2014 13:49	Chase Young	Product Marketing	InfoLock	Member Alert Response Time	Business Intelligence	Robert Tenney
104524	02/20/2014 16:19	Kalyani Pattabandla	Information Technology	(b)	Please integrate QMetry with	(b) (3), Quality Assurance (P&T)	N/A
104551	02/21/2014 09:06	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104553	02/21/2014 09:09	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (medium)	Information Security	Michael Hoffman
104554	02/21/2014 09:11	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104555	02/21/2014 09:11	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (medium)	Information Security	Michael Hoffman
104557	02/21/2014 09:15	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104558	02/21/2014 09:17	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (critical)	Information Security	Michael Hoffman
104559	02/21/2014 09:26	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104560	02/21/2014 09:26	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (medium)	Information Security	Michael Hoffman
104561	02/21/2014 09:28	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (low)	Information Security	Michael Hoffman
104562	02/21/2014 09:30	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104563	02/21/2014 09:34	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (medium)	Information Security	Michael Hoffman
104564	02/21/2014 09:40	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104566	02/21/2014 09:42	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104567	02/21/2014 09:45	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104568	02/21/2014 09:47	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (medium)	Information Security	Michael Hoffman
104570	02/21/2014 09:54	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Java Updates (high)	Systems Engineering	(b)(3):6(f), (b)(4)
104571	02/21/2014 10:02	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (critical)	Systems Engineering	N/A
104573	02/21/2014 10:05	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104576	02/21/2014 10:23	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (critical)	Information Security	Michael Hoffman
104589	02/21/2014 12:43	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED CIFS NULL Session Permitted - (high)	Information Security	Michael Hoffman
104591	02/21/2014 12:51	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED IP Source Routing (high)	Information Security	Michael Hoffman
104593	02/21/2014 12:56	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED IRDP (critical)	Information Security	Michael Hoffman
104594	02/21/2014 13:01	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED IP Source Routing (high)	Information Security	Michael Hoffman
104595	02/21/2014 13:07	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (critical)	Information Security	Michael Hoffman
104721	02/24/2014 11:54	(b)(3):6 (f),(b)(4)	Business Operation	Batch Jobs (BATCH)	New Choice Promo Code	Product Owner	N/A
104724	02/24/2014 12:06		Business Operation	Product Configurator	Promo Code Created Under Wrong Partner in Product Configurator	Product Owner	N/A
104737	02/24/2014 13:01	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Files or directories with no real owner or group (low)	Information Security	Michael Hoffman
104755	02/24/2014 13:33	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Files or directories with no real owner or group (low)	Information Security	Michael Hoffman
104801	02/24/2014 16:05	Mathew Stein	P&T Infrastructure	Linux OS Issues	Nagios Alert for DBA Team - Change emails	Systems Engineering	(b)(3):6
104806	02/24/2014 16:39	(b)(3):6(f),	Finance/Accounting	Batch Jobs (BATCH)	2/20/2014 - Renewal Letter File Failure with Emdeon	N/A	Mala Rakhecha
104811	02/24/2014 21:13	Marco Maldonado	PMO	Other	2 VM servers that will work as load injectors for Performance/load testing	Systems Engineering	Michael Glenney
104939	02/26/2014 14:03	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR (wiki.lifelock.com- Confluence) Security Updates (critical)	Release Team	Aimee Henshaw
104940	02/26/2014 14:06	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR (crucible.lifelock.com Crucible) Security Update (critical)	Release Team	Aimee Henshaw
104946	02/26/2014 14:22	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (high)	Information Security	Michael Hoffman
104964	02/26/2014 14:46	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR REDACTED Security Updates (medium)	Information Security	Michael Hoffman
104965	02/26/2014	Michael Hoffman	Infrastructure	Vulnerability Remediation	VRR REDACTED	Information Security	Michael Hoffman

	14:46			Requests	Security Updates (high)		
104974	02/26/2014 14:55	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Updates (high)	Information Security	Michael Hoffman
105142	02/27/2014 17:52	(b)(3):6(f),	Member Services - Team 3	(b)(3):6(f),	Incidents Not Populating	Middleware (WebLogic) Support	N/A
105176	02/28/2014 10:47	Michael Hoffman	Infrastructure	Vulnerability Remediation Requests	VRR [redacted] Security Update (critical)	Release Team	Aimee Henshaw
105205	02/28/2014 13:20	(b)(3):6	Member Operations	Mobile SMS	Unable to receive Start Text	Application Production Support	(b)(3):6(f),
105231	02/28/2014 16:39	Angela Shanahan	PMO	Website Access	Please add ININ contact center platform URLs to our web proxy server, and allow access	Information Security	Austin Appel

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __51__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

From: Jenner Holden [/O=LIFELOCK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=JENNER.HOLDEN]
Sent: Friday, November 16, 2012 8:01 AM
To: Gwen Ceylon
Subject: Re: RA

I agree, but...

Stop by today. Let's discuss.

Jenner Holden
Director of Information Security | **LifeLock® - Relentlessly Protecting Your Identity™**
480.457.2008 Office | (b)(6),(b)(7)(C) Cell
Jenner.Holden@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

From: Gwen Ceylon <Gwen.Ceylon@lifelock.com>
Date: Thursday, November 15, 2012 7:30 PM
To: Jenner Holden <jenner.holden@lifelock.com>
Subject: RA

I just looked at your RA worksheet. This is a Tony thing, isn't it?

RA, under NIST anyways, isn't about making a long laundry lists of any and every threat and vulnerability conceivable through a brainstorming exercise and stack ranking yourselves against them by applying number values based on how you think you would do if that situation ever happened to arise.

I had to operate under NIST at CGI because being under contract with our Government customer they required us to follow their government processes. Read NIST 800-30 rev 1 – it's changed a lot since the 2002 version you all referenced during the last PCI audit. Also NIST 800-37.

Under the NIST framework the items that went into my RA spreadsheet were actual control gaps found in the environment that had a real need to be evaluated, prioritized and remediated (or not, depending on resources) – like:

1) problems identified during a DR/CP exercise or IR test (or from actual restore/recovery and IR scenarios) that resulted in significantly inadequate performance that could or did adversely impact operations.
2) vulnerabilities and weaknesses found in a pen test or vulnerability scan that are a more systemic problem rather than a quick patch or config change to fix the vulnerability (ie, Windows team refuses to patch systems manually, SCCM and WSUS are both broke so vulnerabilities are increasing in number putting the company at greater risk).
3) missing security controls – ie, not having an app scanner to check in-house developed applications for vulnerabilities or weaknesses.
4) well defined change management plan not in place, people are not following the process, and frequency of (b)(3):6(f) service disruptions is increasing.
5) material weaknesses and deficiencies found in audits – a qualification finding related to user access controls because periodic account reviews are not being performed at all wither manually or with an automated tool to do it.
6) deficiencies or non-compliance found in a security assessment for a project or new deployment of some product or service

7) new compliance requirements that will now need to be met – all public companies need to place cameras in the workplace to continuously monitor, collect fingerprints and retina scans from all employees as a result of an Obama E.O. Nark on Fellow Citizens to Aid DHS in Apprehending and Transporting Dissidents to FEMA CAMP ACT, punishable by sending all executives to do battle with robotic gladiators at the National Amphitheater.
8) technology rendered obsolete and needs replacement – REDA can now be easily broken with publically available exploit code and 2048 bit keys are now longer sufficient so we need to move all systems to REDA and 4096 bit keys across the environment (or as is the case of MD5 and use of LM here at LifeLock).

This is walk the talk kind of stuff – really going out and finding the gaps in the environment rather than find a bunch of threat/vulnerability pairs companies face as examples out on the Internet and making a RA check list of them for LifeLock.

Do you agree?

Gwen Ceylon, CISSP CISM CISA
Contractor - Information Security/Compliance
480.457.2101 Office | (b)(6),(b)(7)(C) Cell
gwen.ceylon@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281
LifeLock® - Relentlessly Protecting Your Identity™

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __52__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

From: (b)(3):6(f),(b)(4)
Sent: Tuesday, March 19, 2013 1:36 PM
To: Scott Watson; David Bridgman
Cc: Chris Ebright; (b)(3):6(f),(b)(4)
Subject: InfoSec Scans

Importance: High

Hi Scott,

Thank you for the call today. I spoke with Dave, and you may have spoken with Chris as well.

Dave and I discussed and Information Security will do a scan on the new systems from the New Cluster Landscape project once in Stage, and then AFTER it has been fully cutover in Production. This is different than what we had discussed earlier. Dave would like to have the scan run after it is fully operational in the production environment.

Chris – InfoSec will need a ticket (or tickets if you are not ready to provide Prod info yet) on a request for a scan and the IPs of the system(s) that will be in Stage, and then in Prod.

Chris and (b)(3):6(f), (b)(4) as part of security best practice (and as part of PCI compliance) InfoSec will need to scan/review all major changes implemented in the environment. While this has not occurred consistently in the past, we are putting steps in place to ensure that the scans are part of the process. Since this is not fully documented and a process vetted (as to what works best in reality) I am asking for a ticket for a scan request at this time. Information Security is working with (b) 'Renee on what the best process will be, not just for your team, but for all Infrastructure and Engineering teams when major changes occur.

Dave, you will need to turn around the scan results quickly, with any remediation that is required for vulnerabilities. I would suggest that any critical or high vulnerabilities be remediated, or an exception requested and reviewed/approved, before going live in Production.

Again, thank you everyone for ensuring scans are being completed.

To Recap Next Steps:

(b)(3):6(f),(b)(4)

Thank you! Please feel free to provide comments or questions.

(b)(3):6(f),(b)(4)

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __53__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

From: (b)(3):6(f),(b)(4)
Sent: Thursday, July 25, 2013 11:10 AM
To: AnneMarie Olson; Austin Appel
Subject: Final Thoughts/Comments/Info

This email is just to brain dump some last items, so the info does not walk out the door with me. Mostly related to PCI.

(b)(3):6(f),(b)(4)

3) Change Management – one thing LL is really lacking is having significant changes scanned after they go into production. I recommend that the change group (gail's group) also be include to ensure that a post-implementation task be assigned to infosec. Austin, if you get a request to scan something that went into production make certain that the task is on a change record. That is where the auditor will look for it and it will be easier to track there.

(b)(3):6(f),(b)(4)

I think that is it although if I think of anything else I certainly will email.

Thank you to you both for making my time at LL very pleasurable. It was great to work with such a talented, dedicated people such as yourselves!

(b)(3):6(f),(b)(4)

Information Security Consultant | LifeLock® - Relentlessly Protecting Your Identity™

(b)(3):6(f),(b)(4)

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __54__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

From: (b)(3):6(f),(b)(4)
Sent: Tuesday, February 11, 2014 10:06 AM
To: AnneMarie Olson
Subject: RE: Change Management Standard

yep

From: AnneMarie Olson
Sent: Tuesday, February 11, 2014 10:03 AM
To: (b)(3):6(f),(b)(4)
Subject: RE: Change Management Standard

(b)(3):6(f),(b)(4)

From: (b)(3):6(f),(b)(4)
Sent: Tuesday, February 11, 2014 9:25 AM
To: AnneMarie Olson
Subject: RE: Change Management Standard

Only one change and I am good.

From: AnneMarie Olson
Sent: Tuesday, February 11, 2014 9:17 AM
To: (b)(3):6(f),(b)(4)
Subject: RE: Change Management Standard

You rock; thanks for quick turn-around and for great input. See changes/comments below and then let me know if we are good.

From: (b)(3):6(f),(b)(4)
Sent: Tuesday, February 11, 2014 8:33 AM
To: AnneMarie Olson
Subject: RE: Change Management Standard

See comments below...

From: AnneMarie Olson
Sent: Monday, February 10, 2014 5:13 PM
To: (b)(3):6(f),(b)(4)
Cc: AnneMarie Olson
Subject: Change Management Standard

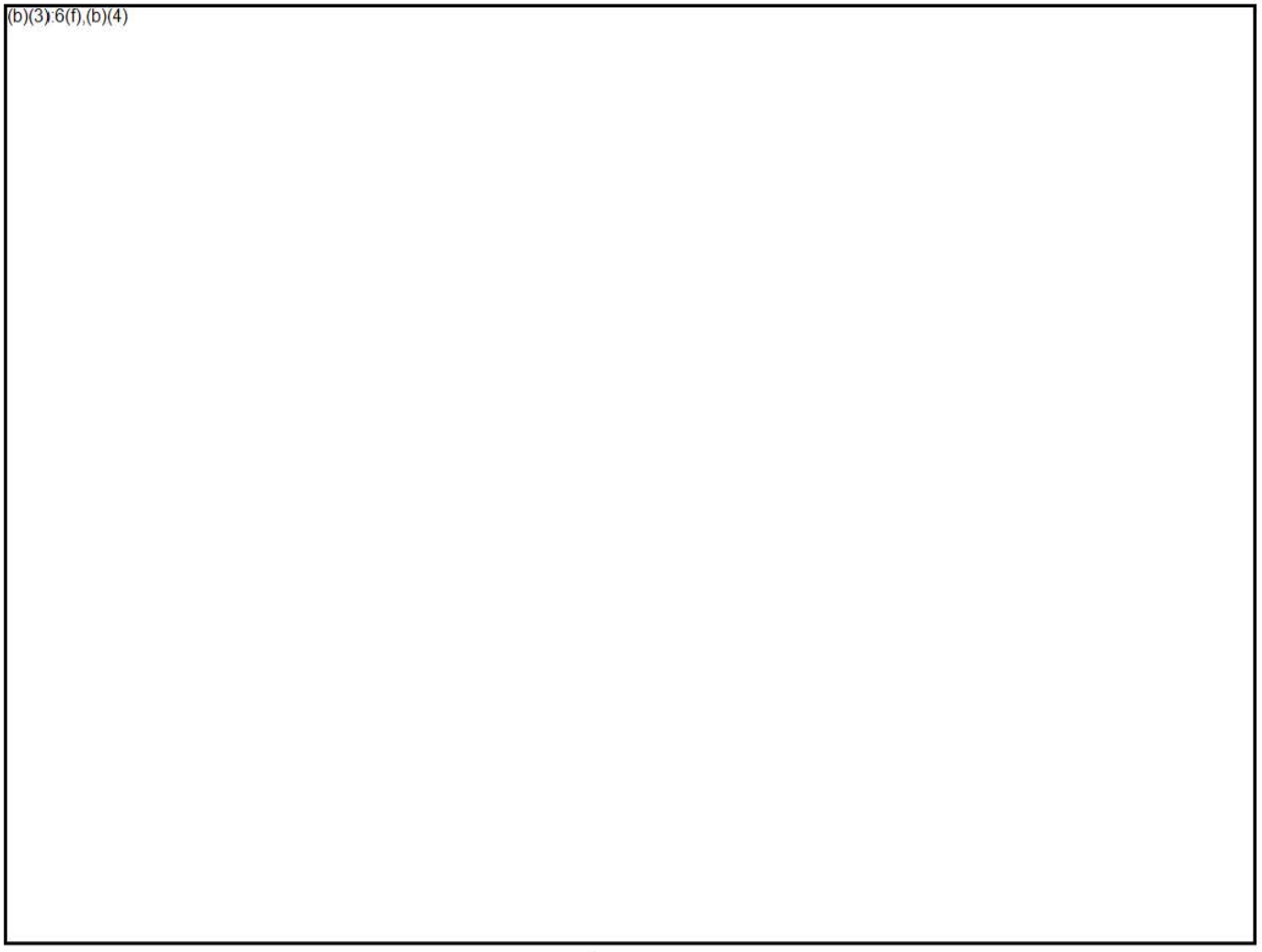
As promised several months ago, I have the standard for change management in final draft. It's part of a larger standard called "Security Standards for Communications & Operations Management." Below is the policy (in red) and the associated standards. Please review with the following objectives in mind:

- Is the standard reasonable and prudent?
- Do we comply with the standard?
  - If yes, could we provide evidence?
  - How do we maintain the compliance?
  - If no, can we comply?
    - If yes, how and when? If remediation is more than 30 days (b)(
    - If no, (b) or change standard

We did the entire document (31 pages) in 4.5 hours so this section shouldn't take longer than an hour or so. I would have set up a separate review meeting with you, but I think we're meeting these in all cases, so this should be a slam dunk. If not, I'm happy to review in person. I'd like to get this back in the next week or so, if possible. Thanks (b) amo

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)



(b)(3):6(f),(b)(4)

Anne Marie Olson (amo) | Information Security | **LifeLock® - Relentlessly Protecting Your Identity™**
480.457.2086 Direct | (b)(6),(b)(7)(C) | annemarie.olson@lifelock.com

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __55__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

From: Tony Valentine [Tony.Valentine@lifelock.com]
Sent: Monday, July 15, 2013 1:13 PM
To: (b)(3):6(f),(b)(4)
Subject: RE: ROC - Updated list of Critical and Post-ROC Items - Version 3

Can you give me a call on this when you can?
Im a bit confused about what you're saying.
Thanks

From: (b)(3):6(f),(b)(4)
Sent: Monday, July 15, 2013 12:12 PM
To: Tony Valentine
Subject: FW: ROC - Updated list of Critical and Post-ROC Items - Version 3
Importance: High

Tony,

Austin is able to do a screenshot of all scans run and dates that they ran. BUT – some of these scans were added after I came in because I had noticed (along with (b) that not all PCI vlans were being scanned.

Now this is going to be noticed by (b) because not all vlans have a year's worth of scans when they should have (b)(3):6(f),(b)(4)

(b) alternative request (DMZ and CDE)....DMZ would be fine but the CDE I think means all the CDE vlans (which is all we scan anyway, and doesn't mean we can remove those vlans that have not been scanned all year)

THOUGHTS?

(b)(3):6(f),(b)(4)

From: (b)(3):6(f),(b)(4)
Sent: Monday, July 15, 2013 11:27 AM
To: (b)(3):6(f),(b)(4)
Cc: (b)(3):6(f),(b)(4) Tony Valentine; (b)(3):6(f),(b)(4) David Bridgman
Subject: Re: ROC - Updated list of Critical and Post-ROC Items - Version 3
Importance: High

Here's the requirement

> 11.2.1.a Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.

I don't need the detailed results of the scans; I just need the report stating a scan was done on a date.

I have a photograph of the screen showing all the VLANS that are scanned. What I don't have is something showing it being done for four quarters.

Will that history show that all 30 VLANS will have been looked at in each of the last four quarters? If so, that will do. If the history is just on one VLAN, then I need the history for each but I will settle for the history of the scans of the DMZ and CDE.

This can be shoved into one file and put in the Infosec folder.

(b)(3):6(f),(b)(

On 15 Jul 2013, at 11:11 AM, (b)(3):6(f),(b)(4) wrote:

Hi (b)(3):6(f

In response to the Internal Vulnerability Scans that Austin performs, there is a level of effort. Can you please read my email to Austin and Austin's response and then let me know what you would prefer?

Thank you!!!

(b)(3):6(f),(b)(4)

From: Austin Appel
Sent: Monday, July 15, 2013 11:07 AM
To: (b)(3):6(f),(b)(4)
Subject: RE: ROC - Updated list of Critical and Post-ROC Items - Version 3

You are correct, we scan by VLAN. Unfortunately, there is no single report that I generate for each report. Here are a few options of things I could do to satisfy the request:

(b)(3):6(f),(b)(4)

From: (b)(3):6(f),(b)(4)
Sent: Monday, July 15, 2013 10:59 AM
To: Austin Appel
Subject: FW: ROC - Updated list of Critical and Post-ROC Items - Version 3

Austin,

How difficult would it be to get this? I believe these scans are not incorporated into one single report, that you scan by vlan. Please let me know the steps and effort and I will speak with (b)(3):6(f

Thank you!

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

From: (b)(3):6(f),(b)(4)
Sent: Monday, July 15, 2013 10:47 AM
To: (b)(3):6(f),(b)(4)
Cc: Suzanne Farr; Tony Valentine; Jeff Weekes; David Bridgman
Subject: Re: ROC - Updated list of Critical and Post-ROC Items - Version 3

I have four quarters of ISV external vulnerabiity scans that I renamed. I don't think I have the internal quarterly reports generated by Austin.

Thanks for the clarification on the PCI tables; I'll adjust my text.

(b)(3):6(f),(b)(4)

On 15 Jul 2013, at 10:39 AM, (b)(3):6(f),(b)(4) wrote:

Please see my comments in **RED**. Also, I am adding Dave to the email.

(b)(3):6(f),(b)(4)

From: (b)(3):6(f),(b)(4)
Sent: Monday, July 15, 2013 10:35 AM
To: (b)(3):6(f),(b)(4)
Cc: Suzanne Farr; Tony Valentine; Jeff Weekes
Subject: Re: ROC - Updated list of Critical and Post-ROC Items - Version 3

Yes, it does help. As I mentioned, I don't see messages that David has posted stuff—maybe this is in a Box setting for him? I will check with Dave on this.

I've searched for the 4 quarters of vulnerability reports and the ad hoc vulnerability report plus ticket for system change you mentioned in an email but I cannot find them.

1) I believe you have the 4 quarters of vulnerability reports because you had renamed them once I had uploaded. Correct?
2) Dave is going to upload these today, if he hasn't already. If he did I will have him send/resend an email as to where this is.

I wrote the compensating controls for access to PCI tables but I have a question and a need. I don't know if you read the paper I sent to Tony and (b)(3):6(f),(b)(4) on this (it's the document *The DSS requirements specifying how access to the database holding CHD is controlled* in the From (b)(3):6(f) folder in the Admin, General folder) but I need to also see a list of non-DBA users who can access the database and the role assigned to them. In my paper (b)(3):6(f),(b)(4) be that broad or did you just mean the encrypted tables? I suggest you put the list of non-DBA users in another tab. Note that I shorten the name and move it to the database folder.

1) I will get you the list of the non-DBA users who have access to the database.
2) (b)(3):6(f),(b)(4)

thanks

(b)(3):

On 15 Jul 2013, at 10:19 AM, (b)(3):6(f),(b)(4) wrote:

Hi (b)(3):6(f)

I will let Tony address the AD comment. **Tony**?

As for the other items you may have missed? I wouldn't know at this point but I am ensuring that Dave and I are also providing you an email when we upload to include location. I certainly hope this helps and if you cannot find something you know or believe has been uploaded in the past, just let me know and I will either find it or upload.

Thanks!

(b)(3):6(f),(b)(4)

From: (b)(3):6(f),(b)(4)
Sent: Friday, July 12, 2013 5:31 PM
To: (b)(3):6(f),(b)(4)
Cc: Suzanne Farr; Tony Valentine; Jeff Weekes
Subject: Re: ROC - Updated list of Critical and Post-ROC Items - Version 3

(b)(3):6(f),(b)(4)

Another misunderstanding on the AD cleanup. I said that Tony had made a note of the bad entries and would fix them along with the other stuff that needs to be fixed. I said I wasn't expecting another AD listing since we suspect that there are more bad entries in AD. Was I wrong in that? Should we get a new list with those errors corrected to reference in the report? We had identified them as things to be corrected and posed to evidence post-RoC.

(b)(3):6(f),(b)(4

On 12 Jul 2013, at 5:02 PM, (b)(3):6(f),(b)(4) wrote:

MY RESPONSES IN RED FOR GAPS OF "DONE" ITEMS.

(b)(3):6(f),(b)(4)

From: (b)(3):6(f),(b)(4)
Sent: Friday, July 12, 2013 4:52 PM
To: Tony Valentine; (b)(3):6(f),(b)(4)
Subject: ROC - Updated list of Critical and Post-ROC Items - Version 3

Please see updates below - Items highlighted in yellow have been received. Also, please see note from (b)(3):6 on contents of Applications Security Assessment report, not sure this if adequate or final version.

On Thu, Jul 11, 2013 at 5:19 PM, (b)(3):6(f),(b)(4) wrote:
All,

With you agreement, I will continue to populate one email with any additional items that have been identified as needed before or after submission. I will coordinate with (b)(3):6(to provide an updated status on each item and include that so we know which items have been dispositioned and which ones are still open. I will provide an update at COB each day so we all have the most current status.

Thanks again and please let me know if there is anything else we can do to assist.

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

* Please see separate email from (b)(3):6(f) regarding document provided for pentest and (b)(3):6(f),(b)(4) Code Review reports.
Regards,

(b)(3):6(f),(b)(4)

"Excellence is not a skill, it is an attitude" - Ralph Marston

(b)(3):6(f),(b)(4) This email message, including any attachments, is for the sole use of the intended recipient (s) and may contain information that is confidential, proprietary, legally privileged, or otherwise protected by law from disclosure. Any unauthorized review, use, copying, disclosure, or distribution is prohibited. If you are not the intended recipient, or the person responsible for delivering this to an addressee, you should notify the sender immediately by telephone or by reply e-mail, and destroy all copies of the original message.

--
(b)(3):6(f),(b)(4)

"Excellence is not a skill, it is an attitude" - Ralph Marston

(b)(3):6(f),(b)(4) This email message, including any attachments, is for the sole use of the intended recipient (s) and may contain information that is confidential, proprietary, legally privileged, or otherwise protected by law from disclosure. Any unauthorized review, use, copying, disclosure, or distribution is prohibited. If you are not the intended recipient, or the person

responsible for delivering this to an addressee, you should notify the sender immediately by telephone or by reply e-mail, and destroy all copies of the original message.

This email message, including any attachments, is for the sole use of the intended recipient (s) and may contain information that is confidential, proprietary, legally privileged, or otherwise protected by law from disclosure. Any unauthorized review, use, copying, disclosure, or distribution is prohibited. If you are not the intended recipient, or the person responsible for delivering this to an addressee, you should notify the sender immediately by telephone or by reply e-mail, and destroy all copies of the original message.

The information contained in this transmission may contain privileged and confidential information. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

This email message, including any attachments, is for the sole use of the intended recipient (s) and may contain information that is confidential, proprietary, legally privileged, or otherwise protected by law from disclosure. Any unauthorized review, use, copying, disclosure, or distribution is prohibited. If you are not the intended recipient, or the person responsible for delivering this to an addressee, you should notify the sender immediately by telephone or by reply e-mail, and destroy all copies of the original message.

The information contained in this transmission may contain privileged and confidential information. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

The information contained in this transmission may contain privileged and confidential information. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

This email message, including any attachments, is for the sole use of the intended recipient (s) and may contain information that is
confidential, proprietary, legally privileged, or otherwise protected by law from disclosure. Any unauthorized review, use, copying,
disclosure, or distribution is prohibited. If you are not the intended recipient, or the person responsible for delivering this to
an addressee, you should notify the sender immediately by telephone or by reply e-mail, and destroy all copies of the original message.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __56__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

KELLEY DRYE & WARREN LLP
A LIMITED LIABILITY PARTNERSHIP

WASHINGTON HARBOUR, SUITE 400
3050 K STREET, NW
WASHINGTON, DC 20007

(202) 342-8400

NEW YORK, NY
LOS ANGELES, CA
CHICAGO, IL
STAMFORD, CT
PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICE
MUMBAI, INDIA

FACSIMILE
(202) 342-8451
www.kelleydrye.com

WILLIAM C. MACLEOD
DIRECT LINE: (202) 342-8811
EMAIL: wmacleod@kelleydrye.com

June 12, 2015

VIA ELECTRONIC MAIL

Susan H. Pope
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mailstop CC-9528
Washington, D.C. 20580

RE: CONFIDENTIAL - LifeLock, Inc.

Dear Susan:

This responds to your letter dated June 9, 2015 and my phone call with Greg of yesterday in which you sought clarification of our June 5, 2015 submission relating to Microsoft and Linux patch histories. After I explained the difficulty of answering questions seeking "all information available," Greg asked if we could at least provide logs and a list of decommissioned servers today. With this letter we are doing that, along with providing answers to other questions that bear on the interpretation of the logs. Please see our responses to your specific questions (repeated in bold typeface) below.

1. The three .csv files you produced (LIFELOCK-0136811, LIFELOCK-0136812, and LIFELOCK-0136813), contain columns with headings and information, with no explanation regarding what the column heading or information means or how it relates to the patching purportedly completed by LifeLock. Accordingly:

a. With respect to .csv file LIFELOCK-0136811:

(1) Provide a detailed description of what is meant by and what information is contained in columns labeled: Change ID; Change Title;Task ID; Title; Description; Created By; Technician; Created Date; Scheduled Start

Time; Task Status; Completed Time; Task Comment; and Comment Time.

The following chart provides descriptions of the column headers:

HEADER	DESCRIPTION
Change ID	Record ID of a change request
Change Title	Title or subject of a change request
Task ID	Record ID of a task record
Title	Title or subject of a task record
Description	Identification of server to be patched
Created By	Technician who created the task record
Technician	Technician to whom the task record was assigned
Created Date	Date/time the task record was created
Scheduled Start Time	Date/time the task was scheduled to start
Task Status	Status of task record
Completed Time	Date/time the task was marked as completed
Task Comment	Comment entered into task record
Comment Time	Date/time comment was entered into task record

(2) For each column, identified in I.a(1), above, describe how the information in each column relates to patching that purportedly was completed by Lifelock.

Change management requests are made to the company's information technology (IT) team to request that patches be installed on various systems. Each change request has an ID and title, and is executed by a technician. Each change request may contain one or more specific tasks to be executed, each which have an ID, status, and start/completion times.

(3) For many cells in the "Completed Time," "Task Comment" columns, there is an entry of "N/A". Please describe what is meant by N/A. For example, with respect to the "Completed Time" column, does "N/A" indicate that the referenced patch(es) were not completed.

We note that LIFELOCK-0136811 supplements the "CR Report 05-13-15" (LIFELOCK-0135782) that was produced to FTC staff on or around May 19, 2015. The "CR Report 05-13-15" log contains the completion time and date for each of the Change Request forms. With respect to LIFELOCK-0136811, the columns "Completed Time" and "Task Comment" were optional data fields. The technician assigned to the task did not need to input a response into

those fields in order for the task to be closed. If the fields were left blank, it would have auto-populated as "N/A." Thus, the notation of "N/A" does not indicate that the referenced patches had not been completed. Moreover, LIFELOCK-0135782 confirms that all Change Request forms that were created in this six-month time period had been completed.

b. With respect to .csv files LIFELOCK-0136812 and LIFELOCK-0136813:

(1) Provide a detailed description of what is meant by and what information is contained in columns labeled: CSName; InstalledOn; HotFixID; Description; Caption; and CVE.

The following chart provides descriptions of the column headers:

LIFELOCK-0136812	
HEADER	**DESCRIPTION**
CSName	The name of the server that received the patch
InstalledOn	Date and time on which the patch was applied on that server
HotFixID	Microsoft Knowledge Base number that corresponds to the vulnerability that was patched
Description	The type of software update ("Security Update" or "Security Update for X" where X denotes the type of browser or server system)
Caption	Link to Microsoft's Knowledge Base website that contains information on the particular vulnerability that was patched
CVE	"Common Vulnerability and Exposure" industry-standard number designated by MITRE, a not-for-profit corporation that works in partnership with government clients and for the public interest (see cve.mitre.org)
LIFELOCK-0136813	
HEADER	**DESCRIPTION**
Server Name	The name of the server that received the patch
Update Package	The name of the file provided by vendor that contains the software update
Installed On Date	Date and time on which the patch was applied on that server
RHSA	"Red Hat Security Advisory Number"
CVE	"Common Vulnerability and Exposure" industry-standard number designated by MITRE, a not-for-profit corporation that works in partnership with government clients and for the public interest (see cve.mitre.org)

(2) For each column, identified in 1.b(1), above, describe how the information in each column relates to patching that purportedly was completed by Lifelock.

The .csv files LIFELOCK-0136812 and LIFELOCK-0136813 were generated by extracting patch history information directly from the servers that were in operation during the six-month time period in question and that still exist in the current environment. See a description of the methodology employed to generate this information in our response to 2(a) below. Each row contained in LIFELOCK-0136812 represents a unique server, identified by the "CSName" field, running Microsoft Windows Server operating systems within the company enterprise. Similarly, each row contained in LIFELOCK-0136813 represents a unique server, identified by "Server Name" running Linux operating systems. The particular patch that was applied to these servers is identified in the "HotFixID" column for Microsoft and the "Update Package" for Linux. The patch application dates are indicated in the respective "Installed On" columns. Finally, the "CVE" column contains the industry CVE rating for the known vulnerability to be patched.

2. In your response you identified and produced two .csv files represented as being LifeLock's (a) Microsoft patch history log (LIFELOCK-0136812), and (b) Linux patch history log (LIFELOCK-0136813) (together, the "patch history logs") for the six month period of September 2012 through March 2013. You further indicated that both of these patch history logs were "pulled directly from the servers still in [Ws] current environment" and that these patch history logs "do[] not include patch histories from servers that were decommissioned in the ordinary course of business."

a. Describe the method by which LifeLock created these two patch history logs (LIFELOCK-0136812 and LIFELOCK-0136813) from the information "pulled directly from the servers."

We pulled patch history data directly from the machines that were in operation during the six-month time period in question and that still exist in the current environment. A company engineer wrote a script to conduct an automated pull of patch histories directly from these machines. This process entailed the development, testing, and deployment of the script on all applicable machines to extract patch history information.

b. Confirm whether these two patch history logs contain all of the available information relating to the patch history of the servers identified. For example, are there other categories of

information on any server relating to its patch history that is not contained on these two patch history logs. If so, describe and produce all available information not contained in these patch history logs.

As I explained in our call yesterday, patch history logs are but one source of information about the patch history of servers. The sources for all available information about the patch history would include the technicians reviewing patches that become available, the technicians involved in testing the applications, those involved in the patching itself, those who recorded the efforts undertaken, those who supervised all these individuals, and others inside and outside ISP who may have knowledge of the circumstances surrounding particular patches. Logs of course provide a useful condensation of information. But they do not provide all the information.

With this letter we are supplementing our prior submissions of logs. Previously we produced the PDFs (LIFELOCK-0135517 – 781) and native files (LIFELOCK-0135784 – 786) for Vulnerability Remediation Requests ("VRR") created between June 2012 through December 2014. These logs contain only the "archived" VRRs that were created during this time period.

We now are producing two logs in native format that contain archived and active, or "work order," VRRs created during a more expansive time frame, April 2012 through May 2015 (LIFELOCK-0138077, LIFELOCK-0138078). To facilitate your review, we are reproducing the entirety of the HTML files associated with the archived VRRs for this time period. We also have included a key that will allow you to match the HTML files to their ticket numbers.

d. With respect to the "decommissioned" servers identified in your response:

(1) Identify all decommissioned servers that were in operation by LifeLock at any time from September 2012 through December 31, 2014;

We are producing a list of the relevant servers that were decommissioned since September 2012 (LIFELOCK-0138076).

Finally, I want to reiterate what I said on the phone yesterday, which is that the information contained in these lists and logs should not be considered definitive. One of the projects that was consuming a great deal of time and resources in the ISP group was to quality-check the information that is reflected in these logs. As we reported last week, the server analysis of the patching activity revealed far more than the over 300 patch applications that we noted in our Commissioner meetings. The over 2,800 we have now identified still significantly understates

the total, because it doesn't include the decommissioned servers. It is probably not important to know the exact number. But the sheer volume of tasks reflected in these logs is a good measure of the difficulty of providing "all information" relating to the activity that these logs reflect, as well as a context for the discussion of the materiality of any individual task.

(2) Provide the dates of operation and decommission of each server identified in 2(d)(1), above; and

We do not have information or documents in our possession, custody, or control that would be responsive to this request.

(3) Provide the Microsoft patch history log(s) and Linux patch history log(s) with respect to each server identified in 2(d)(1), above, that was in operation at any time September 1, 2012 through March 31, 2013.

We do not have information or documents in our possession, custody, or control that would be responsive to this request.

Sincerely yours,

William MacLeod

William C. MacLeod
Sharon Kim Schiavetti

Enclosure

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __57__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

hostname	status	OS	notes
REDACTED	Decom	RHEL 5	Dev (b) Data Warehouse DB Server - VM container name REDACTE
	Decom	CentOS 5	Tomcat Application Server, MYLL, Secure
	Decom	CentOS 5	Tomcat Application Server, MYLL, Secure
	Decom	CentOS 5	Apache Web Server, MYLL, Secure VM container name: REDACTED
	Decom	CentOS 5	Apache Web Server, MyLL, Secure VM container: REDACTED
	Decom	RHEL 4	(b)(3):6 Application Server, WLS, DEV1
	Decom	RHEL 4	(f),(b)(4) Application Server, AP, MyLL, Secure
	Decom	RHEL 4	Application Server, AP, MyLL, Secure
	Decom	RHEL 5	Exchange Big brother serve
	Decom	Windows 2008	Dev Business Objects
	Decom	RHEL 5	Oracle Grid Control / OEM
	Decom	RHEL 4	(b)(3):6(f),(b)(OSB
	Decom	RHEL 5	DEV Oracle Database Server - Member Portal/Enroll/AgentPortal
	Decom	RHEL 5	DEV Oracle Database Server - Member Portal/Enroll/AgentPortal
	Decom	RHEL 5	(b)(3):6(f),(b)(4) - Will impact Introscope monitoring, no impact to business.
	Decom	RHEL 5	- Will impact Introscope monitoring, no impact to business.
	Decom	RHEL 5	- Will impact Introscope monitoring, no impact to business.
	Decom	RHEL 4	Weblogic Application Server, OSB, AP, MyLL, Secure
	Decom	RHEL 4	PRD Weblogic (Member Portal, Enroll, AgentPortal)
	Decom	RHEL 5	Oracle OLAP Server
	Decom	RHEL 5	PRD Oracle Database (Member Portal, Enroll, AgentPortal)
	Decom	RHEL 4	Affiliates Toolbox
	Decom	RHEL 5	Softrax DB Server
	Decom	RHEL 4	QA Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 5	Oracle OLAP
	Decom	RHEL 5	QA Oracle Database Server - Member Portal/Enroll/AgentPortal
	Decom	RHEL 5	QA Oracle Database Server - Member Portal/Enroll/AgentPortal
	Decom	RHEL 5	Red Hat Directory Server
	Decom	RHEL 5	Red Hat Directory Server
	Decom	RHEL 5	STG Apache Member Portal/Enroll
	Decom	RHEL 4	Weblogic Application Server, OSB , AP, MyLL, Secure
	Decom	RHEL 4	Weblogic Application Server, OSB , AP, MyLL, Secure
	Decom	RHEL 4	Weblogic Application Server, OSB , AP, MyLL, Secure
	Decom	RHEL 4	Weblogic Application Server, OSB , AP, MyLL, Secure
	Decom	RHEL 4	Java Batch, Weblogic
	Decom	RHEL 5	PHP Server
	Decom	RHEL 5	(b)(3):6
	Decom	RHEL 5	Oracle Database Server
	Decom	RHEL 5	Oracle Database Server
	Decom	RHEL 4	Windows Teams SSH machine/cron server.
	Decom	RHEL 5	Apache Web Server
	Decom	RHEL 5	Apache Web Server
	Decom	RHEL 5	Apache Web Server
	Decom	RHEL 5	Cron server for APS. ***OLD_DATA - Production ODS database server, provides support for Agent Portal, Member Portal, Webstore, feeds to data warehouse
	Decom	CentOS 5	Tomcat, MyLL, Secure
	Decom	CentOS 5	Tomcat, MyLL, Secure
	Decom	CentOS 5	Tomcat, MyLL, Secure

hostname	status	OS	notes
REDACTED	Decom	CentOS 5	Apache Web Server, MyLL, Secure
	Decom	CentOS 5	Apache Web Server, MyLL, Secure
	Decom	RHEL 5	Oracle Data Warehouse
	Decom	RHEL 5	Oracle Database Server
	Decom	CentOS 5	Tomcat, MyLL, Secure
	Decom	RHEL 4	(b)(3):6(f) Application Server, OSB , AP, MyLL, Secure
	Decom	RHEL 4	PHP Batch Server
	Decom	Windows 2003	smtp server
	Decom	RHEL 5	PRD Apache WWW web, PRD Affiliates Toolbox
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	BO for BI
	Decom	RHEL 5	
	Decom	RHEL 5	QA MySQL server
	Decom	RHEL 5	Business Objects Server
	Decom	RHEL 5	CA CEM Server
	Decom	RHEL 5	CA CEM Server
	Decom	RHEL 5	CA CEM Server
	Decom	Windows XP Pro	Exchange backup mgt
	Decom	Windows 2003	Altiris Ghosting server
	Decom	Windows 2003	CORP Domain Controller
	Decom	Windows 2003	4th St. Aliris
	Decom	Windows 2003	Altiris Deployment Svr
	Decom	Windows 2003	4th St. Print Svr
	Decom	Windows 2003	Speech Analystics Admin Svr - (b)(3):6
	Decom	Windows 2003	Speech Analystics Essentials Svr - (b)(3):6
	Decom	OnTap 7.3.3	Call center filers
	Decom	OnTap 7.3.3	Call center filers
	Decom	Windows 2003	Hayden Ferry CORP Domain Controller
	Decom	Windows 2003	CORP Domain Controller
	Decom	Windows XP Pro	Dev Test box
	Decom	Windows 2003	Hayden Ferry Print Svr
	Decom	Windows 2003	HP Test Director; Dependent on the SQL mounts on REDACTED VM Container name is REDAC
	Decom	Windows 2003	AltirisUtimaco Svr Shutting server down as its no longer needed - 8/17/22
	Decom	Windows 2003	SubCA / AVG Svr
	Decom	Windows 2003	-
	Decom	Windows 2003	(b)(3):6(f),(b) - no impact if rebooted
	Decom	Windows 2003	Lifelock Domain Controller
	Decom	Windows 2003	Lifelock Domain Controller
	Decom	Windows 2003	Lifelock.ad DC
	Decom	Windows 2003	Corp Domain Controller tied to Agent Portal
	Decom	Windows 2003	Win DEV /Test Subversion
	Decom	Windows 2003	Blackberry Enterprise Svr
	Decom	Windows 2003	webmail.lifelock.com - exchange
	Decom	Windows 2003	Exchange MB Store Cluster Node 1
	Decom	Windows 2003	Exchange MB Store Cluster Node 2
	Decom	Windows 2003	Exchange Cluster Node

hostname	status	OS	notes
REDACTED	Decom	OnTap 7.3.3	REDACTED
	Decom	OnTap 7.3.3	REDACTED
	Decom	Windows XP Pro	Monitors Network traffic
	Decom	Windows 2003	MOSS Excel Calculation - Dependent on the SQL mounts on REDACTED
	Decom	Windows 2003	MOSS Search Index - Dependent on the SQL mounts on REDACTED
	Decom	Windows 2003	MOSS Web Front End /Query 01 - Dependent on the SQL mounts on REDACTED
	Decom	Windows 2003	MOSS Web Front End /Query 02 - Dependent on the SQL mounts on REDACTED
	Decom	Windows 2003	Metratech Deployment Svr
	Decom	Windows 2003	NetQOS
	Decom	Windows 2003	(b)(3):6(f),(b)(4) Dependent on the SQL mounts on REDACTED (training team - no impact for patching and reboots)
	Decom	Windows 2003	QA Sharepoint
	Decom	Windows 2003	QA Sharepoint
	Decom	Windows 2003	QA Autosys
	Decom	Windows 2003	ReQlogic GP Purchasing Integration Svr - Dependent on the SQL mounts on REDACTED
	Decom	Windows 2003	Antivirus
	Decom	Windows 2003	Staging Slow Lane Metratech UI/Pipeline
	Decom	Windows 2003	Staging Slow Lane Metratech Activity Servies
	Decom	Windows 2003	Staging Slow Lane Metratech Payment
	Decom	Windows 2008 R2 Std	Citrix Svr 2008 Terminal Svr Licensing
	Decom	Windows 2003	(b)(3): Enterprise Manager (enterprise mgr - affect recording while rebooting)
	Decom	Windows 2003	IP Analyser for (b) (IP recorder - voice recording while rebooting)
	Decom	Windows 2003	(b) (3):6 (f),(b) Quality Monitor (QM recorder - screen recording while rebooting)
	Decom	Windows 2003	Encryption server
	Decom	Windows 2003	Customer Feedback Svr
	Decom	Windows 2008 R2 Std	Prod Citrix Xen App Svr
	Decom	Windows 2008 R2 Std	Citrix Xen App Svr
	Decom	Windows 2003	Wyse ftp
	Decom	Windows 2003	Stage PCI SQL Node 02 - Stage (b)(3):6 (f),(b)(4)
	Decom	Windows 2003	Dev WebSvr
	Decom	Windows 2008 R2 Std	Xen desktop testing
	Decom	Windows 2008 R2 Std	Xen desktop testing
	Decom	Windows 2008 R2 Std	Xen desktop testing
	Decom	Windows 2003	MetraTech QT2
	Decom	Windows 2008 R2 Std	(b)(3):6(
	Decom	Windows 2008 R2 Std	Security Forensics
	Decom	Windows 2003	Exchange
	Decom	Windows 2008 R2 Std	SCCM Secondary
	Decom	Windows 2008 R2 Std	SCOM
	Decom	Windows 2008 R2 Std	Virtural Center
	Decom	Windows 2008 R2 Std	Citrix xen
	Decom	Windows 2008 R2 Std	Citrix xen
	Decom	Windows 2003	QA Autosys
	Decom	Windows 2003	QA HP QC 10
	Decom	Windows 2003	QA New template based on CE & AW gold build for Windows VM's
	Decom	Windows 2008 R2 Std	Stg BO

hostname	status	OS	notes
REDACTED	Decom	Windows XP	Offshore Developer
	Decom	Windows XP	Offshore Developer
	Decom	Windows XP	Offshore Developer
	Decom	Windows XP	Offshore Developer
	Decom	Windows XP	Offshore Developer
	Decom	Windows XP	Offshore Developer
	Decom	Windows XP	Offshore Developer
	Decom	CentOS 5	Spacewalk
	Decom	Other Windows	
	Decom	Other Windows	
	Decom		
	Decom	CentOS 5	NetBackup Linux Media server
	Decom	Windows 2003	(b)(3) Licensing server
	Decom	Windows 2003	(b)(3):6(f),(b)
	Decom	Windows 2003	Stg 2 web server
	Decom	RHEL 5	Grid Control Ok to shut down - This is the production Grid control server. Impacts our database monitoring.
	Decom		
	Decom	Windows 2008 R2 Std	New BES server
	Decom	Windows 2008 R2 Std	Office Lync testing
	Decom	Windows XP	Offshore Developer
	Decom	Windows XP	Offshore Developer
	Decom	Windows XP	Offshore Developer
	Decom	Windows XP	Offshore Developer
	Decom	Windows XP	Offshore Developer
	Decom	Windows XP	Offshore Developer
	Decom	Windows XP	Offshore Developer
	Decom	ESXi 4	4th St ESXi; Backup of guests only
	Decom	ESXi 4.1	Hayen Ferry ESXi
	Decom	ESX 4.1	Dev ESX
	Decom	ESX 4.1	Dev ESX
	Decom	ESX 4.1	Dev ESX
	Decom	ESX 4.1	Dev ESX
	Decom	ESX 4.1	Dev ESX
	Decom	ESX 4	Prod ESX
	Decom	ESX 4	Prod ESX
	Decom	ESX 4	Prod ESX
	Decom	ESX 4	Prod ESX
	Decom	ESXi 4.1	4th St ESXi
	Decom	ESXi 4	Dev ESXi
	Decom	ESXi 4.1	No VMs - standby for DMX
	Decom	ESXi 4.1	No VMs - standby for DMX
	Decom	RHEL 5	STG Apache Member Portal/Enroll
	Decom	RHEL 5	STG Apache Member Portal/Enroll
	Decom	RHEL 5	CA CEM Collector
	Decom	RHEL 5	proxy pass server - www.lifelock.com webserver
	Decom	RHEL 5	proxy pass server - www.lifelock.com webserver

hostname	status	OS	notes
REDACTED	Decom	RHEL 5	Oracle data warehouse db - This is the data warehouse database server. Data Warehouse and Business Objects and Informatica will be unavailable.
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	Oracle Grid Control
	Decom		
	Decom	RHEL 5	Informatica Server
	Decom		
	Decom	Windows 2003	Citrix Licensing server
	Decom		
	Decom	Windows 2003	Altiris package server
	Decom	CentOS 5	Dev Tomcat Member Portal/Enroll VM container name: REDACTED
	Decom	CentOS 5	Dev Tomcat Member Portal/Enroll VM container name: REDACTED
	Decom		
	Decom		
	Decom		
	Decom		
	Decom		
	Decom		
	Decom		
	Decom	Windows 2003	HP Quality Center 10 Server - Sanjay K
	Decom		
	Decom	Windows 2003	Communicator 2007
	Decom	RHEL 4	WebLogic Server
	Decom	RHEL 4	WebLogic Server - B2B Backup
	Decom		
	Decom		prod sep 12 server we are slowly moving toward that server from REDA - is actually
	Decom		
	Decom	Windows 2008 R2 Std	Blackberry admin server - blackberry mai should still flow; safe to reboot
	Decom		
	Decom		
	Decom	Windows XP Pro	(b) Content Producer Server
	Decom		
	Decom	RHEL 4	Dev Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 5	Dev Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 4	Dev Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 4	Dev Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 4	Dev Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 4	Dev Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 4	Dev Weblogic Member Portal/Enroll/AgentPortal
	Decom	CentOS 5	Subversion
	Decom		
	Decom	CentOS 5	Oracle Data Guard
	Decom	CentOS 5	Oracle Data Guard
	Decom	CentOS 5	Oracle Backup Server - backups failing possibly due to vmware tools being out of date
	Decom	CentOS 5	Linux Sendmail Relay

hostname	status	OS	notes
REDACTED	Decom	CentOS 5	Chef Server
	Decom	CentOS 5	
	Decom	Windows 2008 R2 Std	NetBackup Media server
	Decom	CentOS 5	Dev Apache Member Portal/Enroll
	Decom	CentOS 5	Dev Tomcat Member Portal/Enroll
	Decom	RHEL 4	WebLogic Server
	Decom	RHEL 4	WebLogic Server
	Decom	RHEL 4	WebLogic Server
	Decom	CentOS 5	
	Decom	CentOS 5	
	Decom		
	Decom	CentOS 5	UAT Tomcat Member Portal/Enroll
	Decom	CentOS 5	UAT Tomcat Member Portal/Enroll
	Decom	CentOS 5	STG Data Integrator
	Decom	Other Windows	exchange maintenance workstation - BAckups of archived psts only
	Decom	CentOS 5	Tomcat Member Portal/Enroll
	Decom	CentOS 5	Tomcat Member Portal/Enroll
	Decom	CentOS 5	Tomcat Member Portal/Enroll
	Decom	Windows 2008 R2 Std	Used as a WIndows jenkins slave
	Decom	CentOS 5	Agent Proxy RN View Configurator applications. Would impact member services with respect to these applications.
	Decom	CentOS 5	Agent Proxy RN View Configurator applications. Would impact member services with respect to these applications.
	Decom	CentOS 5	Tomcat Member Portal/Enroll
	Decom	CentOS 5	Tomcat Member Portal/Enroll
	Decom	RHEL 4	QT Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 4	QT Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 4	QT Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 4	QT Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 4	QT Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 4	QT Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 4	?
	Decom	Windows 2003	nonprod web server
	Decom	Windows 2003	Dev Citrix
	Decom	Windows 2008	Exchange
	Decom	Windows 2008	Exchange
	Decom	Windows 2008	Citrix server
	Decom	Windows 2008	QT .NET Web server ??
	Decom	Windows 2008	Great Plains Stg
	Decom	CentOS 5	Weblogic Member Portal/Enroll
	Decom	CentOS 5	Weblogic Member Portal/Enroll
	Decom	CentOS 5	Weblogic Member Portal/Enroll
	Decom	CentOS 5	Weblogic Member Portal/Enroll
	Decom	RHEL 5	Jenners tripwire server, used for proof of concept only
	Decom	CentOS 5	Production application support jump box
	Decom	CentOS 5	
	Decom	CentOS 5	
	Decom	CentOS 5	Syslog server test

hostname	status	OS	notes
REDACTED	Decom	Windows 2008 R2 Std	NetBackup Media Server - impacts backups only - if rebooted all netbackup services on REDAC and REDAC have to be restarted
	Decom	Windows 2008	NetBackup Media Server - impacts backups only - if rebooted all netbackup services on REDAC and REDAC have to be restarted
	Decom	CentOS 5	New (b) server
	Decom	Windows XP Pro	
	Decom	CentOS 5	agent proxy sits on this server - We have REDA as a redundant pair.
	Decom	CentOS 5	agent proxy sits on this server - We have REDA as a redundant pair.
	Decom	Windows 2008 R2 Std	vCenter VMware server
	Decom	CentOS 5	Tomcat Member Portal/Enroll
	Decom	Other Windows	
	Decom	Other Windows	
	Decom	Other Windows	
	Decom	Other Windows	
	Decom	Other Windows	
	Decom	Other Windows	
	Decom	Other Windows	QA WebSvr
	Decom	Other Windows	
	Decom	Windows 2008	(b)(3):6(f),(b)
	Decom	Windows 2008 R2 Std	Windows test box
	Decom	Other Windows	
	Decom	Other Windows	
	Decom	Windows 2003	Dev Reqlogic
	Decom	Windows 2008 R2 Std	Fiddler2 web debugger
	Decom	Windows 2008 R2 Std	SQL server
	Decom	Windows 2003	Autosys - Batch jobs wont execute if this system goes offline. Impacts alerts and some fulfillment operations.
	Decom	RHEL 5	Standby database server
	Decom	RHEL 5	Standby database servers
	Decom	CentOS 6	
	Decom	RHEL 5	Softrax DB Server
	Decom	RHEL 5	Need to check VMware Tools, vm backups failing
	Decom	RHEL 5	WebLogic Server
	Decom	RHEL 5	WebLogic Server
	Decom	RHEL 5	WebLogic Server
	Decom	RHEL 5	WebLogic Server
	Decom	RHEL 5	WebLogic Server
	Decom	RHEL 5	WebLogic Server
	Decom	ESXi 4.1	Prod ESX
	Decom	Windows 7	Offshore Dev
	Decom	Windows 2008 R2 Std	SharePoint 2010 sql server
	Decom	Windows 2003	.NET Web server ??
	Decom	Appliance	Firemon for Network
	Decom	RHEL 5	
	Decom	Windows 2008 R2 Std	Windows jump box
	Decom	RHEL 6	
	Decom	RHEL 6	
	Decom	RHEL 4	

hostname	status	OS	notes
REDACTED	Decom	RHEL 6	Weblogic Server -- going to be decommd
	Decom	RHEL 6	
	Decom	RHEL 6	
	Decom	Windows 2003	Prod AP / IIS server
	Decom	Windows 2003	Prod AP / IIS server
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	To possibly be used for all AOL traffic still being decided if were going to bypass the apache layer or not
	Decom	RHEL 4	
	Decom	RHEL 4	
	Decom	RHEL 5	Stage batch
	Decom	RHEL 5	
	Decom	CentOS 5	
	Decom	CentOS 5	
	Decom	RHEL 5	
	Decom	RHEL 6	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	CentOS 5	
	Decom	CentOS 5	
	Decom	CentOS 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	Undefined Linux	
	Decom	Undefined Linux	
	Decom	Undefined Linux	
	Decom	Undefined Linux	
	Decom	Undefined Linux	
	Decom	Undefined Linux	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	

hostname	status	OS	notes
REDACTED	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	RHEL 5	
[redacted]	Decom	Windows 2008 R2 Std	
[redacted]	Decom	Windows 2003	
[redacted]	Decom	Windows 2003	
[redacted]	Decom	Windows 2008 R2 Std	
[redacted]	Decom	Windows 2008 R2 Std	
[redacted]	Decom	Windows 2008 R2 Std	
[redacted]	Decom	Windows 2008 R2 Std	
[redacted]	Decom	Windows 2008 R2 Std	
[redacted]	Decom	Windows 2008 R2 Std	
[redacted]	Decom	RHEL 5	

hostname	status	OS	notes
REDACTED	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	Datacenter Network Management
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	Windows 2003	
	Decom	Windows 2003	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	Windows 2003	
	Decom	RHEL 5	
	Decom	Windows 2003	
	Decom	CentOS 6	(b)(3):6(f),(b) (Security team)
	Decom	Windows 2008 R2 Std	SQL server 2008 -QT
	Decom	RHEL 6	
	Decom	RHEL 6	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom		Chef frontend node
	Decom	RHEL 6	Chef frontend node
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	Windows 2008 R2 Std	
	Decom	Windows 2008 R2 Std	
	Decom	Windows 2008 R2 Std	
	Decom	CentOS 5	Network Sentry
	Decom	Windows 2008 R2 Std	
	Decom	Other Windows	Added by sync script
	Decom	Undefined Linux	Added by sync script
	Decom	Other Windows	Added by sync script
	Decom	Other Windows	Added by sync script
	Decom	Other Windows	Added by sync script

hostname	status	OS	notes
REDACTED	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	Undefined Linux	Added by sync script
	Decom	Undefined Linux	Added by sync script
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	Undefined Linux	Added by sync script
	Decom	Undefined Linux	Added by sync script
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	Undefined Linux	Added by sync script
	Decom	RHEL 5	
	Decom	Undefined Linux	Added by sync script
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom		
	Decom	CentOS 5	Apache Web Server
	Decom	CentOS 5	Apache Web Server
	Decom	RHEL 5	Dev Weblogic Member Portal/Enroll/AgentPortal
	Decom	RHEL 5	
	Decom	Other Windows	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	Other Windows	
	Decom	RHEL 5	
	Decom	Undefined Linux	Added by sync script
	Decom	RHEL 5	

hostname	status	OS	notes
REDACTED	Decom	Other Windows	
	Decom	RHEL 5	
	Decom	RHEL 4	Business Objects, Data Integrator- SERVER IS BEING DECOMMISSIONED
	Decom	Other Windows	
	Decom	Other Windows	
	Decom	Other Windows	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	Other Windows	
	Decom	RHEL 5	proxy pass server - www.lifelock.com webserver
	Decom	RHEL 5	proxy pass server - www.lifelock.com webserver
	Decom	RHEL 5	To possibly be used for all AOL traffic still being decided if were going to bypass the apache layer or not.
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	CentOS 5	
	Decom	CentOS 5	Jenkins - Primary jenkins interface but wont impact the critical application.
	Decom	CentOS 5	Nagios
	Decom	CentOS 5	Weblogic artifact repository
	Decom	RHEL 5	
	Decom	Undefined Linux	
	Decom	RHEL 5	
	Decom	RHEL 6	
	Decom	RHEL 5	logvol info not available due to /dev/cdrom bug.
	Decom	RHEL 5	/dev/cdrom lvdisplay bug.
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 6	Apache
	Decom	RHEL 6	
	Decom	RHEL 6	
	Decom	RHEL 6	
	Decom	Undefined Linux	Added by sync script
	Decom	Undefined Linux	Added by sync script
	Decom	CentOS 5	
	Decom	CentOS 5	STG Tomcat Member Portal/Enroll
	Decom	CentOS 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	
	Decom	RHEL 5	middleware engineering
	Decom	RHEL 4	
	Decom	RHEL 4	
	Decom	RHEL 4	

hostname	status	OS	notes
REDACTED	Decom	RHEL 4	
	Decom	RHEL 4	
	Decom	RHEL 4	
	Decom	Undefined Linux	
	Decom	RHEL 5	
	Decom	Windows 2003	
	Decom	Other Windows	MGMT Jump Box
	Decom	Other Windows	Added by sync script
	Decom	Other Windows	Added by sync script
	Decom	Other Windows	Added by sync script
	Decom	Windows 2008 R2 Std	
	Decom	Other Windows	Added by sync script
	Decom	Other Windows	Added by sync script
	Decom	Other Windows	Added by sync script
	Decom	Other Windows	Added by sync script
	Decom	Other Windows	Added by sync script
	Decom	Other Windows	Added by sync script

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __58__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

From: Patrick Pendleton [/O=LIFELOCK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=PATRICK.PENDLETON]
Sent: Monday, October 01, 2012 9:44 AM
To: Dale Eske
Subject: FW: Q4 Staffing

Pat Pendleton
Chief Information Officer | **LifeLock® - Relentlessly Protecting Your Identity™**
480.457.2027 Office | 480.718.8473 Fax |
patrick.pendleton@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281
(b)(3):6(f),(b)(4)

From: Jenner Holden <jenner.holden@lifelock.com>
Date: Wednesday, September 26, 2012 4:56 PM
To: Patrick Pendleton <patrick.pendleton@lifelock.com>
Subject: Q4 Staffing

(b)(3):6(f),(b)(4)

We do have a few penetration tests every year from external vendors. (b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4) They were very excited about this possibility when I discussed it with them last week.

Let me know if you need any further details.

Additionally – I anticipate needing two (b) (6) in 2013.

- One is for Austin to move to a full-time security analyst, as he will graduate in December.
- One is for transitioning the security analyst contract position t to full-time...If things work out with Gwen.

Jenner Holden
Director of Information Security | **LifeLock® - Relentlessly Protecting Your Identity™**
480.457.2008 Office | (b)(6),(b)(7)(C)
Jenner.Holden@lifelock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __59__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __60__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

From: (b)(3):6(f),(b)(4)
Sent: Wednesday, November 13, 2013 3:22 PM
To: Brian Kao
Subject: Re: Refer-a-Friend Release into Stage

Not a problem! Keep me honest :). It's been a bumpy ride for me without an (b)(3):6 (f),(b)(4) person.

Sent from my iPhone

On Nov 13, 2013, at 3:03 PM, "Brian Kao" <Brian.Kao@lifelock.com> wrote:

> Agree that we need to have formal communication to all Teams, but let's have a quick 15 minute discussion Tomorrow. I am quite surprised by some of the new statements you made, which were not stated during our previous formal discussions.
>
> Brian

From: (b)(3):6(f),(b)(4)
Date: Wednesday, November 13, 2013 2:45 PM
To: Brian Kao <brian.kao@lifelock.com>
Subject: RE: Refer-a-Friend Release into Stage

Brian, I can't right now, in meetings all day.

I really need to get an email written up with the parameters of when to engage InfoSec, which I think will help everyone tremendously vs. just a phone call. That way I am saying the same words to everyone.

Will that work? I still can talk to you though if you would like, it will just need to be tomorrow or Friday. If you do want to talk, can you schedule us 15 minutes on the calendar?

Thank you very much!

(b)(3):6(f),(b)(4)

From: Brian Kao
Sent: Wednesday, November 13, 2013 2:41 PM
To: (b)(3):6(f),(b)(4)
Subject: Re: Refer-a-Friend Release into Stage

(b) (3):6(f)

Please call my ext x0566 when you have the chance. I would like to better understand when PEN test is required so that I can better communicate to the Engineering Team.

Thanks,

Brian

From: (b)(3):6(f),(b)(4)
Date: Wednesday, November 13, 2013 2:32 PM
To: Eileen Kim <Eileen.Kim@lifelock.com>, (b)(3):6(f),(b)(4)
Cc: Andrew Citro <Andrew.Citro@lifelock.com>, Brian Kao <brian.kao@lifelock.com>
Subject: RE: Refer-a-Friend Release into Stage

Refer-a-friend is a code change, with new code/functionality presented in the external facing Web that accepts input.

If the marketing pages are also accepting input then we will need to discuss performing the same reviews to ensure that there are not critical vulnerabilities causing risk.

I hope that information helps Eileen. Again, this is part of ensuring InfoSec activities are more appropriately embedded in the SDLC process.

As for the marketing pages, let's have a phone conversation to discuss those in more detail to understand the changes that are made and thus I can better determine the infosec level of effort needed. Would you mind if I setup something in a couple of weeks? I can have this group in that meeting.

(b)(3):6(f),(b)(4)

From: Eileen Kim
Sent: Wednesday, November 13, 2013 11:00 AM
To: (b)(3):6(f),(b)(4)
Cc: Andrew Citro; Brian Kao
Subject: RE: Refer-a-Friend Release into Stage

Hi (b)(3):6(f),
Please advise what the pen test is for. Refer a friend will live in the member portal. We have a landing page on www associated with it but we create landing pages for marketing purposes all the time. We have never had to run a pen test for these types of changes before.

I'll set up meeting as well to understand.

Thanks
Eileen

From: (b)(3):6(f),(b)(4)
Sent: Wednesday, November 13, 2013 8:25 AM
To: Eileen Kim; (b)(3):6(f),(b)(4)
Cc: Andrew Citro
Subject: Refer-a-Friend Release into Stage

Good Morning Eileen and (b)(3):6(f), (b)(4)

Yesterday Andrew attended the meeting for refer-a-friend in my place. He has indicated that you are preparing to move it into stage.

(b)(3):6(f),(b)(4)

Thank you so much everyone!

Cristy Schaan
CISO | **LifeLock® - Relentlessly Protecting Your Identity™**
480.457.2091 Office | 480.200.8676 Cell
Cristy.schaan@LifeLock.com
60 E. Rio Salado Parkway, Suite 400, Tempe, AZ 85281

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __62__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document.**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __63__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document.**

GT GreenbergTraurig

Andrew G. Berg
Tel 202.331.3181
Fax 202.331.3101
berga@gtlaw.com

March 11, 2015

Gregory Madden, Esq.
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mailcode: CC-9528
Washington, DC 20580

Re: LifeLock, Inc.

Dear Mr. Madden:

This responds to your request letters dated February 6 and 18, 2015. We have set forth the requested information as set forth in your letters. (Please note that your questions are set forth below in bold typeface).

Questions 1 and 2 (February 6, 2015 Request):

1. LifeLock Membership List

Please identify all LifeLock members during the period of October 1, 2012 through March 31, 2014. Include in that identification the following information for each member: name, telephone number(s), email address(es), and mailing address(es).

I have confirmed that the requested materials were submitted on March 9th via upload to the FTC's ftp site under separate cover.

2. LifeLock Enrollments and Revenues

Please provide, for the January 1, 2012 through December 31, 2014 time period, an identification of enrollments and revenues attributable to a particular marketing promotion, advertisement, or promotion code, including, but not limited to any, television, newspaper, Internet, radio, or direct mail advertising, marketing promotion, or promotion code.

Include in your response, using your previously identified advertisement reference numbers found in LIFELOCK-0133784-792, an identification of the enrollments and revenues associated with each of the advertisements included on LIFELOCK-0133784-792.

For the same time period, identify the enrollments and revenues that are not attributable to a particular marketing promotion, advertisement, or promotion code.

Please see the enrollment and revenue schedule set forth at Annex 2 (this supplements the enrollment and revenue schedule submitted to you by letter dated February 19, 2015).

Question 3 (February 18, 2015 Request):

As we discussed yesterday, the FTC is interested in what actions, if any, LifeLock has taken related to the concerns the FTC identified in its January 5, 2015 settlement correspondence. Specifically, please describe the actions LifeLock has taken with respect to:

(1) LifeLock's compliance with Permanent Injunction Section I.A as it relates to LifeLock's identity theft protection service monitoring and alert notification claims;

(2) LifeLock's compliance with Permanent Injunction Section II as it relates to establishing, implementing, and thereafter maintaining a comprehensive information security program; and

(3) LifeLock's compliance with Permanent Injunction Section VIII.A.7 as it relates to maintaining all records and documents necessary to demonstrate full compliance with the Permanent Injunction.

Include in your response LifeLock's actions, if any, related to the concerns identified in the correspondence, that occurred prior to, as well as after, January 5, 2015. Please identify the dates any such actions occurred.

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

Please advise whether you have any questions regarding the foregoing; please accord the foregoing information confidential treatment under the Commission's Rules of Practice.

Very truly yours,

Andrew Berg
A.B.

Andrew G. Berg
Counsel to LifeLock, Inc.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __64__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document.**

LIFELOCK RESPONSE TO FTC 3/13/14 INFORMATION REQUEST -- CONFIDENTIAL TREATMENT REQUESTED

1. Identify and describe each component of LifeLock's "proactive alert system."

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

5. Describe any instances, not identified in response to Specification No. 4, where LifeLock delayed or suppressed any alert for any period of time. Include within your description, the types of alerts, the number of alerts involved, the number of customers involved, and the dates of each instance.

Specifications 5 and 8 are very closely related; therefore, the responses to these two Specifications are combined below in the response to Specification 8.

8. Describe any instances where LifeLock engaged in "smoothing out" alerts. Include within your description, the types of alerts, the number of alerts involved, the number of customers involved, and the dates of each instance.

In order to address these issues, it is important to understand the steps followed by LifeLock in processing the alerts and notifications for our members. In addition, this provides an explanation of the circumstances where, on limited occasions, LifeLock was unable to process the alerts or where an alert or notification was delayed by LifeLock for an amount of time that was outside the normal time required to process the alerts and notifications.

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

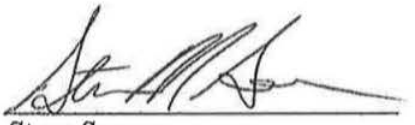
FTC PROPOSED EXHIBIT __65__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

SWORN ATTESTATION OF STEVE SEOANE

I, Steve Seoane, hereby swear and attest that I have personal knowledge of the facts described in the declaration attached at Exhibit A hereto, the contents of which are incorporated by reference as if set forth in full herein. All of the facts set forth in my declaration attached as Exhibit A are true and correct. If called upon to testify, I could and would do so competently to all of the facts set forth in my declaration attached as Exhibit A.

The undersigned certifies, under penalty of perjury pursuant to 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on March 6, 2015



Steve Seoane

EXHIBIT A

DECLARATION OF STEVEN SEOANE

1. My name is Steven Seoane. My address at my place of employment is 60 E. Rio Salado Parkway Suite 400 Tempe, AZ 85281. My place of employment is LifeLock, Inc. My current employment position is as the Chief Product Officer for LifeLock and job responsibilities at LifeLock are to oversee the product management, product development, user experience, and design for the company's products. I started in this role in February of 2013. Prior to my role as the Chief Product Officer of LifeLock, I was the Senior Vice President of Enterprise Solutions for ID Analytics a San Diego based wholly owned subsidiary of LifeLock with an address at 15253 Avenue of Science, San Diego, CA 92128. I served in this role for approximately 18 months. Over the twelve years prior to joining ID Analytics I held various executive product, analytics, and engineering roles at LexisNexis Risk Solutions, and Capital One Financial. My educational background is as follows: I graduated from the United States Naval Academy in 1993 with a Bachelor of Science degree and I graduated from the University of Maryland with a Masters of Business Administration in 2000.
2. In conjunction with the FTC's investigation of LifeLock, I have been involved in the preparation of responses to the FTC's information and data requests and assembling material and data in response thereto. More specifically, I have reviewed LifeLock's responses to the FTC's information and data requests and I am generally knowledgeable of the allegations made by the FTC in the proposed findings as received by the company on January 5, 2015.
3. (b)(3):6(f),(b)(4)
4.
5.

(b)(3):6(f),(b)(4)

6.

7.

8.

9.

10

(b)(3):6(f),(b)(4)

11. I have reviewed LifeLock's responses to the FTC's data and information requests that are relevant to this issue. In particular, I reviewed LifeLock's responses dated March 31st, 2014, April 7th, 2014, July 21st 2014, August 12th 2014, August 15th 2014, and October 28th, 2014. Nothing in those responses is contrary to my statements set forth above in these paragraphs. Unfortunately, I attribute the allegations made by the FTC in the proposed findings to a misunderstanding of the facts set forth in those responses by LifeLock.

12 (b)(3):6(f),(b)(4)

13.

(b)(3):6(f),(b)(4)

Executed on March 6, 2015

Steven Seoane

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __67__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document.**

GT GreenbergTraurig

Andrew G. Berg
Tel 202.331.3181
Fax 202.331.3101
berga@gtlaw.com

July 2, 2014

Gregory Madden, Esq.
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mailcode: CC-9528
Washington, D.C. 20580

Re: LifeLock, Inc.

Dear Mr. Madden:

This responds to your letter dated June 16th 2014 in which you made follow-up inquiries to our submissions dated March 31st and April 7th 2014 relating to the timing and transmission of alerts and notifications by LifeLock to its members. We have set forth the requested information following the order of your requests in your letter.

(b)(3):6(f),(b)(4)

GT GreenbergTraurig

(b)(3):6(f),(b)(4)

Question 13:
For each instance of system maintenance or unplanned system outage, provide the number of LifeLock customers signed up for such alerts at that time.

Response:
The spreadsheet providing alert gap analysis (at Annex 3) lists the number of alerts that potentially were delayed along with the number of unique LifeLock customers that potentially might have been impacted. Also, as noted above, we believe this to be the best available estimate of potential consumer impact.

Questions related to weekend processing of EWS alerts

Question 14: (Page 3)
Did LifeLock "receive" the EWS alerts on the identified weekends?

Response:
No, LifeLock did not "receive" the EWS alerts on the identified weekends. Rather, these alerts were held by EWS.

Question 15: (Page 3)
If not, describe why the alerts were not received on the identified weekends? Include in your answer LifeLock's role, if any, in LifeLock not receiving the EWS alerts.

Response:
As described in our March 31st and April 7th responses and during our January 17th meeting with you, these alerts were "carried over" through the identified weekends because of the specific circumstances related to these alerts. These alerts typically were delivered to LifeLock in high volumes and many of them only reported bank "internal" administrative events; furthermore, the EWS systems did not distinguish between bank-generated and user-generated actions. In addition, these were not "real time" alerts. Moreover, LifeLock was concerned this might create an adverse customer experience due to potentially extended queue times in member services over the weekend. Accordingly, LifeLock instructed EWS to delay the transmission of such alerts to LifeLock over these weekend time periods.

GREENBERG TRAURIG, LLP ▪ ATTORNEYS AT LAW ▪ WWW.GTLAW.COM
2101 L Street NW, Suite 1000 ▪ Washington, DC 20037 ▪ Tel 202.331.3100 ▪ Fax 202.331.3101

GT GreenbergTraurig

(b)(3):6(f),(b)(4)

Please accord the foregoing information and enclosed materials confidential treatment under the Commission's Rules of Practice.

Very truly yours,

Andrew G. Berg

Andrew G. Berg
Counsel to LifeLock, Inc.

GREENBERG TRAURIG, LLP ▪ ATTORNEYS AT LAW ▪ WWW.GTLAW.COM
2101 L Street NW, Suite 1000 ▪ Washington, DC 20037 ▪ Tel 202.331.3100 ▪ Fax 202.331.3101

Annex 18

EWS Alerts - List of Weekends where alerts were not processed

Label	Start Date	Start Time	End Date	End Time	Potential Duration (in hrs)	# of Alerts Processed	# of Members Impacted	Notes	GAP_START MEM_COUNT	GAP_END MEM_COUNT
Alert Gap	10/12/2012	7:00 PM	10/15/2012	7:00 AM	61	0		Weekend alerts not processed	1677491	1680288
Alert processed after gap	10/15/2012	8:00 AM				502	464			
Alert Gap	11/2/2012	6:00 PM	11/5/2012	7:00 AM	62	0		Weekend alerts not processed	1723296	1726202
Alert processed after gap	11/5/2012	8:00 AM				363	328			
Alert Gap	11/9/2012	6:00 AM	11/12/2012	7:00 AM	62	0		Weekend alerts not processed	1734657	1738692
Alert processed after gap	11/12/2012	8:00 AM				165	158			
Alert Gap	11/16/2012	5:00 PM	11/19/2012	7:00 AM	63	0		Weekend alerts not processed	1748272	1750936
Alert processed after gap	11/19/2012	8:00 AM				506	475			
Alert Gap	11/23/2012	5:00 PM	11/26/2012	7:00 AM	63	0		Weekend alerts not processed	1760500	1763303
Alert processed after gap	11/26/2012	8:00 AM				234	220			
Alert Gap	11/30/2012	6:00 PM	12/3/2012	7:00 AM	62	0		Weekend alerts not processed	1774594	1777313
Alert processed after gap	12/3/2012	8:00 AM				315	291			
Alert Gap	12/7/2012	6:00 PM	12/10/2012	8:00 AM	63	0		Weekend alerts not processed	1786457	1788806
Alert processed after gap	12/10/2012	9:15 AM				444	426			
Alert Gap	12/14/2012	6:00 PM	12/17/2012	7:00 AM	62	0		Weekend alerts not processed	1797063	1799176
Alert processed after gap	12/17/2012	8:00 AM				353	347			
Alert Gap	12/21/2012	5:00 PM	12/24/2012	7:00 AM	63	0		Weekend alerts not processed	1808945	1811310
Alert processed after gap	12/24/2012	8:00 AM				302	265			
Alert Gap	12/28/2012	6:00 PM	12/31/2012	7:00 AM	62	0		Weekend alerts not processed	1818268	1820818
Alert processed after gap	12/31/2012	8:00 AM				371	331			
Alert Gap	1/4/2013	6:00 PM	1/7/2013	7:00 AM	62	0		Weekend alerts not processed	1829782	1832526
Alert processed after gap	1/7/2013	8:00 AM				425	384			
Alert Gap	1/11/2013	6:00 PM	1/14/2013	7:00 AM	62	0		Weekend alerts not processed	1843130	1846162
Alert processed after gap	1/14/2013	8:00 AM				343	319			
Alert Gap	1/18/2013	6:00 PM	1/21/2013	7:00 AM	62	0		Weekend alerts not processed	1857584	1860410
Alert processed after gap	1/21/2013	8:00 AM				374	334			
Alert Gap	1/25/2013	5:00 PM	1/28/2013	7:00 AM	63	0		Weekend alerts not processed	1870871	1874266
Alert processed after gap	1/28/2013	8:00 AM				88	86			
Alert Gap	2/1/2013	6:00 PM	2/4/2013	7:00 AM	62	0		Weekend alerts not processed	1885519	1888621
Alert processed after gap	2/4/2013	8:00 AM				439	411			
Alert Gap	2/8/2013	6:00 PM	2/11/2013	7:00 AM	62	0		Weekend alerts not processed	1901233	1904828
Alert processed after gap	2/11/2013	8:00 AM				522	473			

Alert Gap	2/15/2013	6:00 PM	2/18/2013	7:00 AM	62	0		Weekend alerts not processed (incl	1916500	1920187
Alert processed after gap	2/18/2013	8:00 AM				512	475			
Alert Gap	2/22/2013	6:00 PM	2/25/2013	7:00 AM	62	0		Weekend alerts not processed	1932006	1935772
Alert processed after gap	2/25/2013	8:00 AM				355	299			
Alert Gap	3/1/2013	6:00 PM	3/4/2013	7:00 AM	62	0		Weekend alerts not processed	1949299	1954295
Alert processed after gap	3/4/2013	8:00 AM				167	157			
Alert Gap	3/8/2013	6:00 PM	3/11/2013	7:00 AM	62	0		Weekend alerts not processed	1969175	1973350
Alert processed after gap	3/11/2013	8:00 AM				166	149			
Alert Gap	3/15/2013	6:00 PM	3/18/2013	6:00 AM	61	0		Weekend alerts not processed	1986366	1990428
Alert processed after gap	3/18/2013	7:45 AM				85	80			
Alert Gap	3/22/2013	6:00 PM	3/25/2013	7:00 AM	62	0		Weekend alerts not processed	2003197	2006815
Alert processed after gap	3/25/2013	8:00 AM				480	455			
Alert Gap	3/29/2013	6:00 PM	4/1/2013	7:00 AM	62	0		Weekend alerts not processed	2019029	2022357
Alert processed after gap	4/1/2013	8:00 AM				377	356			
Alert Gap	4/5/2013	6:00 PM	4/8/2013	7:00 AM	62	0		Weekend alert not processed	2034354	2037405
Alert processed after gap	4/8/2013	8:00 AM				467	450			
Alert Gap	4/12/2013	6:00 PM	4/15/2013	7:00 AM	62	0		Weekend alerts not processed	2051285	2055931
Alert processed after gap	4/15/2013	8:00 AM				226	216			
Alert Gap	4/19/2013	6:00 PM	4/22/2013	7:00 AM	62	0		Weekend alerts not processed	2068659	2072342
Alert processed after gap	4/22/2013	8:00 AM				96	94			
Alert Gap	4/26/2013	5:00 PM	4/29/2013	7:00 AM	63	0		Weekend alerts not processed	2084302	2088039
Alert processed after gap	4/29/2013	8:00 AM				427	410			
Alert Gap	5/3/2013	6:00 PM	5/6/2013	7:00 AM	62	0		Weekend alerts not processed	2100119	2103598
Alert processed after gap	5/6/2013	8:00 AM				365	338			
Alert Gap	5/10/2013	6:00 PM	5/13/2013	7:00 AM	62	0		Weekend alerts not processed	2115609	2118594
Alert processed after gap	5/13/2013	8:00 AM				423	403			
Alert Gap	5/17/2013	6:00 PM	5/20/2013	7:00 AM	62	0		Weekend alerts not processed	2129628	2133121
Alert processed after gap	5/20/2013	8:00 AM				326	292			
Alert Gap	5/24/2013	6:00 PM	5/28/2013	7:00 AM	86	0		Weekend alerts not processed	2143911	2148433
Alert processed after gap	5/28/2013	8:00 AM				383	373			
Alert Gap	5/31/2013	6:00 PM	6/3/2013	7:00 AM	62	0		Weekend alerts not processed	2156924	2161250
Alert processed after gap	6/3/2013	8:00 AM				341	314			
Alert Gap	6/7/2013	6:00 PM	6/10/2013	7:00 AM	62	0		Weekend alerts not processed	2172559	2175909
Alert processed after gap	6/10/2013	8:00 AM				252	216			
Alert Gap	6/14/2013	6:00 PM	6/17/2013	7:00 AM	62	0		Weekend alerts not processed	2186846	2189828
Alert processed after gap	6/17/2013	8:30 AM				22	22			
Alert Gap	6/21/2013	5:00 PM	6/24/2013	7:00 AM	63	0		Weekend alerts not processed	2201141	2204379

Alert processed after gap	6/24/2013	8:00 AM				340	328			
Alert Gap	6/27/2013	5:00 PM	7/1/2013	8:00 AM	88	0		Weekend alerts not procssed (Incl p	2212897	2219179
Alert processed after gap	7/1/2013	9:30 AM				31	29			
Alert Gap	7/5/2013	5:00 PM	7/8/2013	6:00 AM	63	0		Weekend alerts not processed	2228705	2231967
Alert processed after gap	7/8/2013	8:00 AM				285	269			
Alert Gap	7/19/2013	6:00 PM	7/23/2013	7:00 AM	86	0		Weekend alerts not processed	2257416	2262983
Alert processed after gap	7/23/2013	8:00 AM				558	499			
Alert Gap	8/2/2013	7:00 PM	8/5/2013	9:00 AM	63	0		Weekend alerts not processed	2287211	2290802
Alert processed after gap	8/5/2013	10:45 AM				308	306			
Alert Gap	11/1/2013	7:00 PM	11/4/2013	8:00 AM	62	0		Weekend alerts not processed	2501493	2505851
Alert processed after gap	11/4/2013	9:45 AM				209	198			
Alert Gap	11/8/2013	7:00 PM	11/12/2013	6:00 AM	84	0		Weekend alerts not processed (Incl	2518875	2524572
Alert processed after gap	11/13/2013	7:15 AM				74	74			
Alert Gap	11/24/2013	8:00 AM	11/27/2013	8:00 AM	73	0	0	Partial Weekend (Includes Planned	2554739	2562169
Alert processed after gap	11/27/2013	9:00 AM				195	187			

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __68__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

LifeLock, Inc.
Internal Audit

2013 Internal Audit Plan

2/21/2013

2013 Annual Plan – Table of Contents

- **2013 Audit Plan Overview**
- **Internal Audit's Risk Assessment Process**
  - Overview of Audit Risk Assessment Process
  - List of Risk Categories
  - Top Enterprise Risks by Category Grouping
  - Top Auditable Sorted Risks
- **2013 Audit Plan**
  - 2013-2014 Audit Calendar
  - 2013-2014 SOX Timeline
  - KPMG 2013 Planned SOX Coverage
- **2013 Department Objectives**

LifeLock

2013 AUDIT PLAN OVERVIEW

Internal Audit (IA) is pleased to present the 2013 risk assessment and internal audit plan. The plan identifies the prioritized activities and efforts audits of IA anticipates beginning or completing during 2013. The plan reflects the viewpoints Internal Audit gathered during its recently completed annual risk assessment process.

2013 AUDIT PLAN KEY FEATURES

- ❑ FY 2013 Audit Plan is aligned with the company's top strategic initiatives and is risk-based to focus on the higher, critical risk areas.
- ❑ All of the risk factors, as reported in the S1 registration statement, are identifiable to the risk universe.
- ❑ 2013 will be primarily focused on completing the annual PCI-DSS compliance audit in the first half of the year and completing the execution of the SOX 404 requirements, including remediation in the last half of the year.
- ❑ The execution of SOX 404 assumes resources from KPMG to a) ensure comprehensive SOX coverage and b) increased assurance that important issues stemming from PCAOB are addressed for E&Y signoff.
- ❑ 2013 also represents the formal build out and progression of the audit function for execution in 2014 and beyond. The build out consists of identifying and refining the audit universe, granulizing auditable risks, refining the risk assessment process, defining current vs. future state of controls and evaluating resource requirements.
- ❑ Internal Audit plans to provide project management oversight for the PCI audit and SOX 404 program; as well as overseeing the design and construction of controls within the company's new billing system implementation project.

LifeLock, Inc.
Internal Audit

IA's Risk Assessment Process


(b)(3):6(f),(b)(4)

RISK UNIVERSE

In order to identify the preliminary risk universe, Internal Audit (IA) began the process by listing the top risks (as perceived by internal audit) in each of the following areas – strategy, operations, compliance, finance and IT.

Source: Corporate Executive Board, Financial Leadership Exchange

Strategic	Operational	Compliance	Financial	Information Technology
S1. Governance	O1. Sales and marketing	C1. Standards of conduct	F1. Liquidity	(b)(3):6(f),(b)(4)
S2. Planning & Allocation	O2. Member Services	C2. Legal	F2. Accounting & Reporting	
S3. Major Initiatives	O3. Purchasing & Supply	C3. Regulatory	F3. Tax	
S4. Brand & Communication	O4. People/Human Resources		F4. Capital	
	O5. Fulfillment		F5. Market	
	O6. Assets		F6. Internal Control Over Financial Reporting	

LifeLock

LIFELOCK-0051795-6

TOP ENTERPRISE RISKS – BY GROUPING

TYPE	Auditable Risks			Likelihood	Impact	Velocity	Complexity	Control Maturity	Overall Risk Score
	SOURCE	RISK	REF	0.25	0.25	0.10	0.15	0.25	
STRATEGIC	Governance	Lack of overall governance, no tone at top, lax control environment, no consistent rules or standards	S1	2	2	2	3	3	2.40
	Planning & Allocation	No formal org structure, ad hoc annual budgets, no strategic planning, poor technical development	S2	1	3	2	3	3	2.40
	Major Initiatives	No vision, direction, poor planning and execution, poor technical implementations, trouble in M&A, poor targets, poor due diligence, no process improvement, no measures or monitoring, no business acceptance, poor execution or integration	S3	3	3	3	3	2	2.75
	Brand & Communication	No brand policy or standards, poor customer relations, no crisis communications for bad press, poor corporate image or reputation	S4	2	3	3	2	2	2.35
OPERATIONAL	Sales & Marketing	Poor pipeline management, poor marketing programs, poor revenue management, pricing strategies, lack of systems	O1	3	3	2	2	2	2.50
	Member Services	Inefficient or poor member experience, workforce management, poor outsourcing, lack of systems or processes	O2	2	3	2	3	2	2.40
	Purchasing & Supply	No planning or forecasting, no procurement strategies, lack of systems, vendor management, no cost control or reductions or synergies, no explicit approvals or authorizations	O3	2	2	2	2	3	2.25
	People/Human Resources	No clear culture or culture change management, lack of qualified skills, resources, no training or awareness, recruiting and retention issues, comp and benefit management, incentives, contractors	O4	2	2	2	2	2	2.00
	Fulfillment	Lack of formal controls to ensure all billed customers fulfilled and all fulfilled customers have been billed	O5	3	3	2	3	2	2.65
	Assets	Poor records of assets, equipment, maintenance, facility management	O6	2	1	2	2	2	1.75

TOP ENTERPRISE RISKS – BY GROUPING cont'd

				Likelihood	Impact	Velocity	Complexity	Control Maturity	Overall Risk Score
	SOURCE	RISK	REF	0.25	0.25	0.10	0.15	0.25	
COMPLIANCE	Conduct	No formal policies on standards of conduct, ethics or fraud prevention, company policy violations	C1	2	2	1	2	2	1.90
	Legal	Lack of contracting process, controls and contract management, lack of contracting database, lack of security and privacy programs, unprotected IP, lack of data classification and retention and disposal, no risk management program	C2	3	2	2	3	3	2.65
	Regulatory	Lack of regulatory compliance (FTC, FCC, SEC, PCI, SOX, DOL), data breach guidelines, tax compliance, advertising compliance	C3	2	4	2	3	3	2.90
FINANCIAL	Liquidity	Poor cash management, poor credit & collection processes, poor investment strategies, inadequate insurance protections/reserves,	F1	2	2	1	2	2	1.90
	Accounting & Reporting	Financial reporting weaknesses, poor data integrity in systems, poor billing & collections, payroll fraud, poor disclosures in filings, spreadsheets, policies and procedures	F2	3	3	2	3	2	2.65
	Tax	No tax strategies or accurate reporting, sales and use tax in states, income tax provisions, returns and tax reserves, lack of resources and expertise	F3	3	3	2	2	2	2.50
	Capital	No access to debt, equity financing	F4	2	2	1	2	2	1.90
	Market	Impact of credit rating on interest and cost of capital	F5	2	2	1	2	2	1.90
	Internal Control Over Finl Reporting	SOX deficiencies and material weaknesses, lack of ownership or resources	F6	3	3	2	3	3	2.90

LIFELOCK-0051795-8

TOP ENTERPRISE RISKS – BY GROUPING cont'd

				Likelihood	Impact	Velocity	Complexity	Control Maturity	Overall Risk Score
	SOURCE	RISK	REF	0.25	0.25	0.10	0.15	0.25	
INFO TECHNOLOGY	(b)(3):6(f),(b)(4)								

TOP AUDITABLE RISKS – SORTED

TYPE	SOURCE	AUDITABLE RISK	REF	Weight
IT	(b)(3):6(f),(b)(4)			
COMP	**Regulatory**	**Lack of regulatory compliance (FTC, FCC, SEC, PCI, SOX, DOL), data breach guidelines, tax compliance, advertising compliance**	**C3**	**2.90**
FINL	**Internal Control Over Finl Reporting**	**SOX deficiencies and material weaknesses, lack of ownership or resources**	**F6**	**2.90**
IT	(b)(3):6(f),(b)(4)			
IT				
IT				
IT				
STRAT	Major Initiatives	No vision, direction, poor planning and execution, poor technical implementations, trouble in M&A, poor targets, poor due diligence, no process improvement, no measures or monitoring, no business acceptance, poor execution or integration	S3	2.75
COMP	Legal	Lack of contracting process, controls and contract management, lack of contracting database, lack of security and privacy programs, unprotected IP, lack of data classification and retention and disposal, no risk management program	C2	2.65
OPER	Fulfillment	Lack of formal controls to ensure all billed customers fulfilled and all fulfilled customers have been billed	O5	2.65
FINL	Accounting & Reporting	Financial reporting weaknesses, poor data integrity in systems, poor billing & collections, payroll fraud, poor disclosures in filings, spreadsheets, policies and procedures	F2	2.65

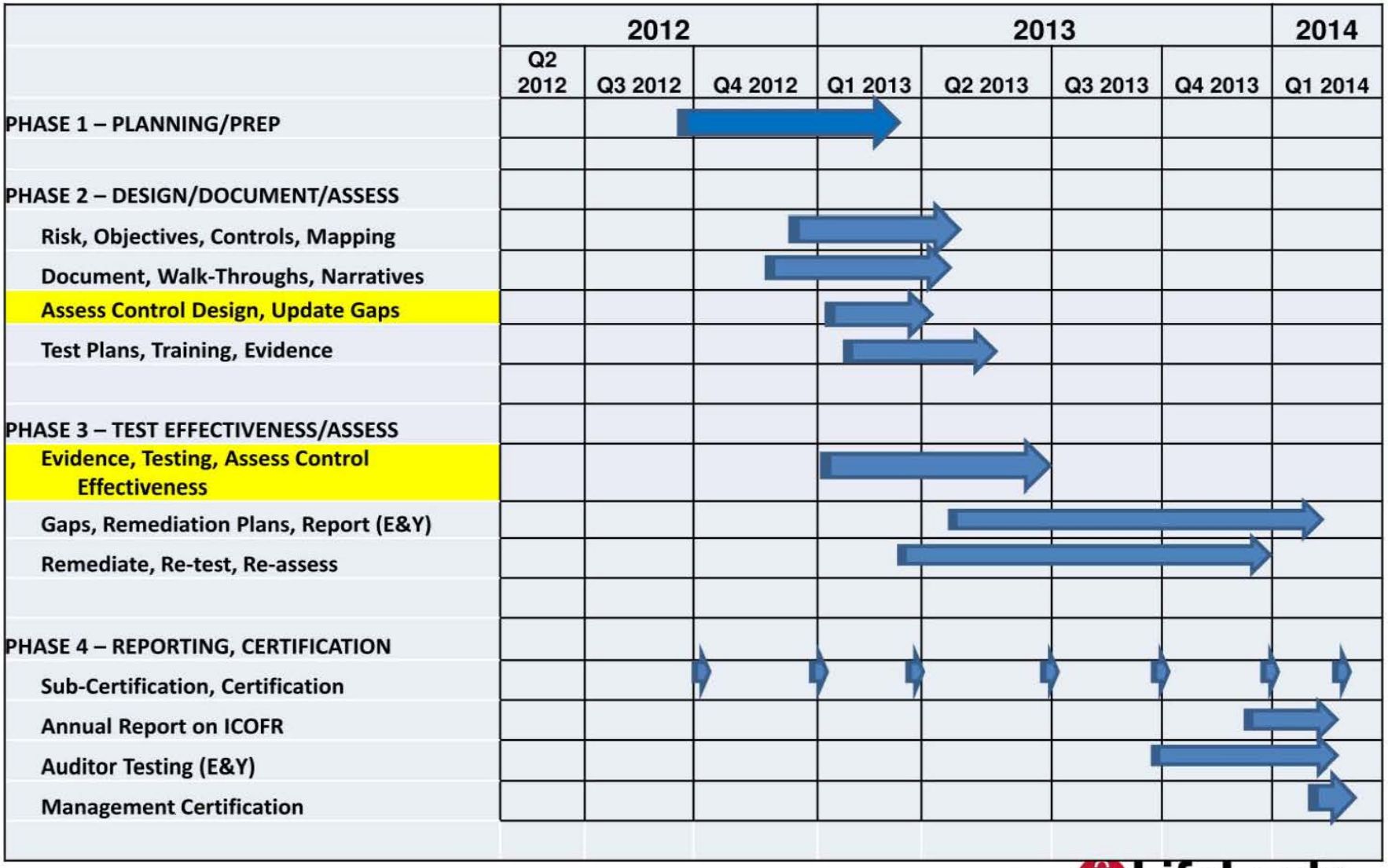
TOP AUDITABLE RISKS – SORTED cont'd

TYPE	SOURCE	AUDITABLE RISK	REF	Name Weight
OPER	Sales & Marketing	Poor pipeline management, poor marketing programs, poor revenue management, pricing strategies, lack of systems	O1	2.50
FINL	Tax	No tax strategies or accurate reporting, sales and use tax in states, income tax provisions, returns and tax reserves, lack of resources and expertise	F3	2.50
IT	(b)(3):6(f),(b)(4)			
IT				
STRAT	Governance	Lack of overall governance, no tone at top, lax control environment, no consistent rules or standards	S1	2.40
STRAT	Planning & Allocation	No formal org structure, ad hoc annual budgets, no strategic planning, poor technical development	S2	2.40
OPER	Member Services	Inefficient or poor member experience, workforce management, poor outsourcing, lack of systems or processes	O2	2.40
STRAT	Brand & Communication	No brand policy or standards, poor customer relations, no crisis communications for bad press, poor corporate image or reputation	S4	2.35

TOP AUDITABLE RISKS – SORTED cont'd

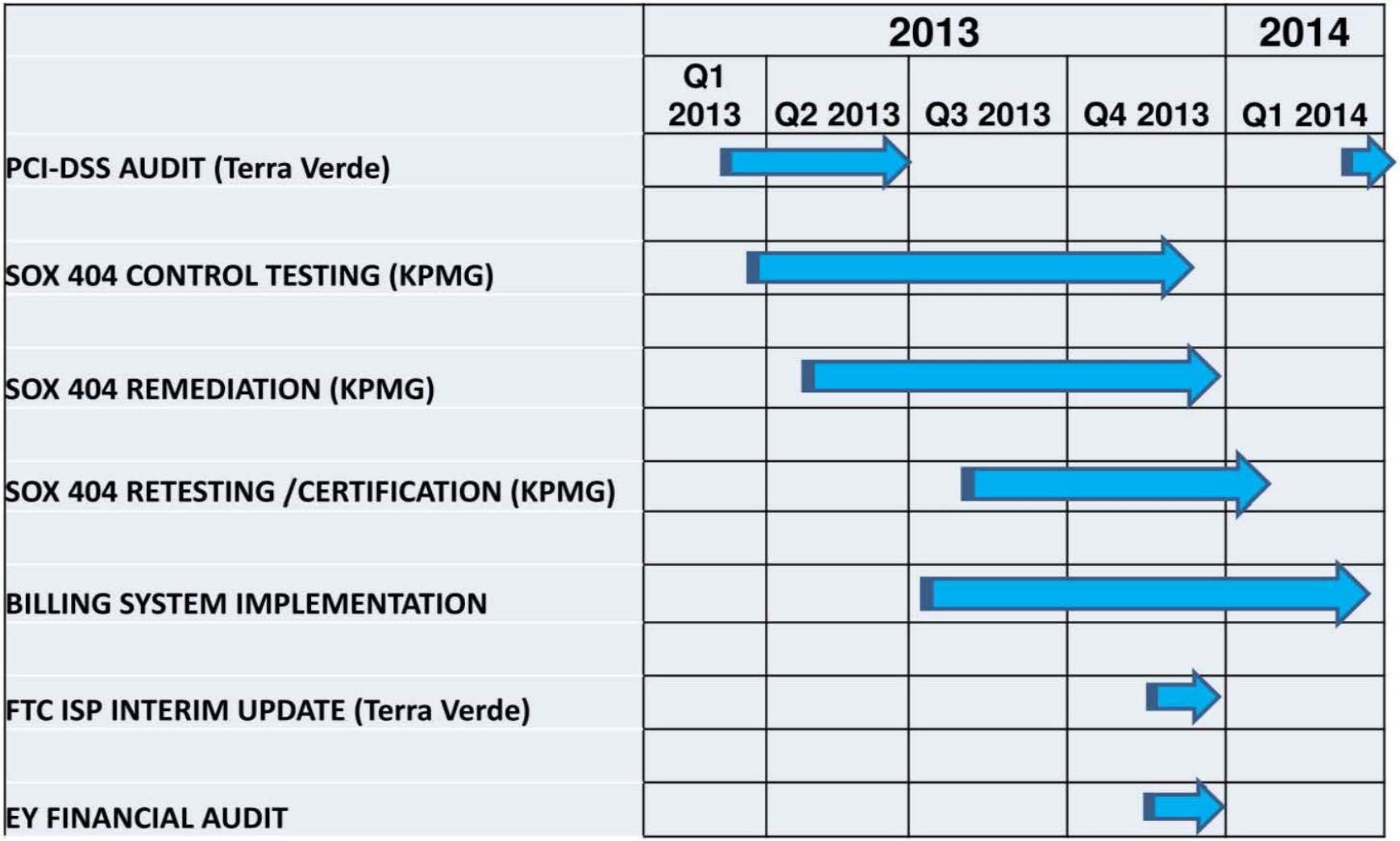
TYPE	SOURCE	AUDITABLE RISK	REF	Name Weight
OPER	Purchasing & Supply	No planning or forecasting, no procurement strategies, lack of systems, vendor management, no cost control or reductions or synergies, no explicit approvals or authorizations	O3	2.25
IT	(b)(3):6(f),(b)(4)			
IT				
IT				
OPER	People/Human Resources	No clear culture or culture change management, lack of qualified skills, resources, no training or awareness, recruiting and retention issues, comp and benefit management, incentives, contractors	O4	2.00
COMP	Conduct	No formal policies on standards of conduct, ethics or fraud prevention, company policy violations	C1	1.90
FINL	Liquidity	Poor cash management, poor credit & collection processes, poor investment strategies, inadequate insurance protections/reserves,	F1	1.90
FINL	Capital	No access to debt, equity financing	F4	1.90
FINL	Market	Impact of credit rating on interest and cost of capital	F5	1.90
OPER	Assets	Poor records of assets, equipment, maintenance, facility management	O6	1.75

SOX TIMELINE



LifeLock

2013-2014 AUDIT CALENDAR



LifeLock

Upcoming Events, Milestones

PCI Audit

- Required annual audit per PCI-DSS for level 1 merchant
- Compliant Report of Compliance (ROC) – remediate until compliance
- Due date to acquirer/processor is approximately June 30, 2013

- Kick off Meeting held 2/19
- P&T management working on readiness efforts and as gap analysis
- Audit approach will be on non-infrastructure areas first; then infrastructure

- Anticipating leverage of PCI controls into SOX control narratives for Q2, Q3
- Issues/Challenges
  - P&T infrastructure environment preparing for changes in Q1
  - All current, new changes will be in scope for testing
  - If any remediation, it could delay ROC, require extensions

LifeLock

Upcoming Events, Milestones

SOX Readiness for 2013

- Internal Audit (IA) is not charged with responsibility for preparing documentation for SOX compliance – this continues to remain with the business units in order to maintain independence

- IA has provided the following:
  - Performed initial risk assessment and FS mapping to scope SOX segments
  - Created repositories for documentation accumulation and storage by business units;
  - Assisted in discussions with business units on rationalization and identification of key controls;
  - Provided guidance and assistance to business units on how to flow from process > controls > evidence > walkthrough > testing
  - Summarized and assessed documentation for overall readiness and testing

(b)(3):6(f),(b)(4)

(b)(3):6(f),(b)(4)

2013 AUDIT DEPARTMENT OBJECTIVES

- 1) IA will help deliver continued compliance and a certified Report of Compliance (ROC) under the PCI-DSS audit.
- 2) IA will execute and deploy the necessary resources and management involvement to complete its SOX 404 documentation and testing, and to deliver an unqualified report with no material weaknesses through 2013.
- 3) IA will complete the formal build out and progression of the audit function for execution in 2014 and beyond. The build out consists of identifying and refining the audit universe, granulizing auditable risks, refining the risk assessment process, defining current vs. future state of controls and evaluating resource requirements.
- 4) Each of the top 4 “sorted” auditable risks identified, will be touched and assessed within the 2013 audit plan to ensure monitoring and assessment of these high, critical risk areas.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __69__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

From: Gwen Ceylon [/O=LIFELOCK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=GWEN.CEYLON]
Sent: Thursday, December 20, 2012 10:34 AM
To: Tony Valentine
Subject: 2012 RA Workbook - Update 12192012.xlsx
Attachments: 2012 RA Workbook - Update 12192012.xlsx

Close to final. Jenner giving it another read.

BTW, he wanted to take out everything that is not P&Ts and really he wanted to take out everything that wasn't specifically Security Team's function.

Doing this reduces this down to something other than an overall company-wide, business risk assessment/compliance program, and removes risk items that P&T could potentially offer solutions for. Ie, employee dissatisfaction in Member Services (a 2011 item). If it's due to systems and applications that suck so bad they can't do their jobs how will awareness be brought to that issue if we aren't more comprehensive in our RA approach.

I can't say I agree with this approach. If this is reduced down to just security teams stuff then who's going to be accountable/responsible for the rest? You? That's the suggestion.

“Instructions” worksheet

(b)(3):6(f),(b)(4)

“RA Type 2012” worksheet

	Risk ID #	Information Asset Type	Risk	Threat	Vulnerability	Source	Security Concern	SOX	PCI	FTC	Probability	Impact	Risk Areas				Initial Risk	Chance of Detection/ Prevention	Risk Priority Number	Risk Rating	Controls	Residual Risk Rating	Notes/ References
		Information, Hardware, Software, Physical Assets, People, Services					C = Conf I = Integrity A = Avail				L: = 0.1 M: = 0.5 H: = 1.0	L: = 10 M = 50 H: = 100	Financial	Operations	Legal / Regulatory	Member Loyalty	Prob X Imp L = 0-10 M = 25, 50 H = 100	Very easy = 1 Relatively easy = 2 Effort needed = 3 Low likelihood = 4 Very difficult = 5	Risk X Chance of Detection	L: = 0 - 49 M: = 50-199 H: = 200 - 500	Controls to mitigate/reduce risk	Final risk rating after controls	
1	1	Information (Member Data)	LOSS, THEFT OR DISCLOSURE OF MEMBER SENSITIVE DATA	Unauthorized access leading to theft and/or loss.	1) Unclear access control processes/procedures. 2) Access control process/procedure not followed or is circumvented. 3) Terminated/inactive users are not identified and disabled/removed. 4) Improper access control (user access) review.	Quarterly account review. Assessment of system monitoring configurations.	C, I	x	x	x	1.0	100	x	x	x	x	100	4	400	High		High	
5	2	Information (Member Data)		Compromise of Administrative-level Authentication Credentials giving unauthorized privileged access to systems.	Using unsecure communications protocols which pass authentication credentials in the clear (i.e., unencrypted RDP to Windows 2003 Servers [redacted]).	Continuous vulnerability scanning	C, I		x		0.5	100		x			50	4	200	High	[redacted]	Medium	Very easy to fix, and should be considered for remediation.
6	3	Information (Member Data)		Unauthorized access and potential for system compromise and information loss.	Using weak cipher algorithms, weak keys, encryption that has been successfully hacked (i.e., MD5, SSH Protocol version 1, 56-bit encryption, RSA keys with key length of 1024 bits or less), and vendor supplied self-signed certificates.	Continuous vulnerability scanning	C, I		x		0.5	100		x			50	4	200	High		Medium	
9	4	Information (Member Data)		Loss, theft, tampering or disclosure of member sensitive data by 3rd Party service provider and vendors.	Weaknesses in Vendor Management processes.	Annual review of vendor list showing it is not up to date with current list of vendors.		x	x		0.1	100.0		x			10	4	40	Low		Low	
11	5	Information (Member Data)		Unauthorized access leading to theft and/or loss.	Weaknesses in access control to systems and ineffective monitoring.	Number of findings from default accounts on systems found in vulnerability scans to system configuration settings to events captured in monitoring tools.	C, I	x	x	x	1.0	50	x	x	x	x	50	4	200	High		High	
12	6	Hardware	HARDWARE UNAVAILABILITY	Hardware not monitored	Weaknesses in security monitoring for performance, capacity and operational incidents. Deficient HW/SW maintenance program.	On-going Infrastructure Stabilization issues. Critical systems operating on unsupported EOL versions of software/firmware.	I A	x	x	x	0.5	100	x	x	x	x	50	3	150	Medium		Medium	
14	7	Hardware		Failure of hardware/systems - INT	Weakness in DRP, BCP	Out of date Infrastructure BCP/DRP. Place has not been tested since 2009.	I A	x	x	x	0.5	100	x	x	x	x	50	3	150	Medium		Medium	
15	8	Hardware		Unauthorized or sabotaged changes to hardware	Lack of standard configurations and build lists for critical components; Lack of proper change control, approvals. Weaknesses in file integrity monitoring	Missing configuration standards for system components. Changes circumventing change control management procedure. Weaknesses in FIM.	C I A	x	x	x	0.5	50	x	x	x		25	3	75	Medium		Medium	
8	9	Hardware		Hardware/systems Outage - INT	Inefficient incident response causing excessive delay in restoration, no defined Service Level Agreements, outdated BCP, and lacking DRP and IR plans. No annual testing of plans.	Service outage due to firmware upgrade and response time length before services restored.	A	x	x		1.0	100.0	x	x	x	x	100	2	200	High	Issue pertains to P&T Operations and can impact business services - not directly related to information security or PCI.	Medium	
2	10	Software	SOFTWARE FUNCTIONALITY AND PERFORMANCE	Exploit poorly configured systems exposed to the internet could result in an intruder gaining access to networks and systems.	Incorrect Security configuration setting allows directory traversal in an externally facing web application such that when exploited it can reveal highly sensitive information giving an attacker information they can use to penetrate and further exploit the network.	Annual Pen Test	C, I, A	x			1.0	100		x			100	2	200	High	[redacted]	Medium	
16	11	Software		"Hackers" (external or internal) attempt to exploit possible system vulnerabilities to gain access to member data or crash systems.	Lack of 24/7 network and security monitoring staff to respond to hacker attempts.	Observation	C, A	x			0.5	50	x	x	x	x	25	2	50	Medium	Implemented Alert Logic early December.	Low	
10	12	Software		Exploit of any of the high number of vulnerabilities can put the company's business operations at risk.	High number of vulnerabilities, particularly critical and exploitable vulnerabilities, on systems in the PCI environment.	Vulnerability trends and stats from vulnerability scan reports.	C, I, A	x	x	x	1.0	100.0		x			100	3	300	High		High	
13	13	Physical Assets	LOSS, THEFT OR DISCLOSURE OF PHYSICAL ASSETS	Assets used to support member operations are not identified or recorded	Lack of controls to ensure diligence in performing asset inventory	Out of date and incomplete asset inventory.	I	x	x		1.0	50	x		x		50	3	150	Medium		Medium	
4	14	People	SUPPLY AND/OR BEHAVIOR OF PEOPLE	Well crafted phishing attacks can potentially result in loss of sensitive information and compromise of user authentication credentials.	Unsuspecting users reveal sensitive information and their userIDs/passwords to an attacker.	Annual User Testing of Policy Control regarding Phishing Attacks. On-going testing shows that employees still fall for phishing schemes.	C, I, A	x			1.0	50		x		x	50	4	200	High	Started implementing phishing tests to train and educate users.	High	
	15	People		Unauthorized access to member data terminated employees or employees changing positions	Weaknesses in employee termination process	Accounts of terminated employees still active on systems.	C	x	x	x	0.5	50		x	x	x	25	3	75	Medium		Medium	
	16	People		Breach of security (social engineering, physical security breach) resulting in theft of member data	Lack of security awareness	Employees are continuing to loose LL equipment (laptops) and fall for phishing attacks.	C	x	x	x	1.0	100	x	x	x	x	100	4	400	High	New security training program.	Medium	
7	17	Services	INSECURE, UNAUTHORIZED OR IMPROPER SERVICES	Loss of services due to system changes occurring in production without first having been tested in development.	Stage, QA and Dev environments are used for testing of key elements, but not all changes are tested in these environments first.	Sev 1 Incident Reporting	C, I, A	x	x		1.0	100		x			100	2	200	High	Project underway to improve testing environments as part of the Infrastructure Stabilization project.	High	
3	18	Services		Introduction of compatibility issues and unresolvable security vulnerabilities which can be exploited putting the infrastructure at risk of service interruptions and various possible compromises.	Running operating systems and firmware in the environment (RHEL 4, Cisco) which have reached EOL, are no longer maintained or supported by the vendor, can no longer be patched, and are potentially causing integration issues [redacted] Feb 2012).	Continuous vulnerability scanning	A	x	x		1.0	100		x			100	1	200	High		High	

“Sorted RPN 2012” worksheet

	Risk ID #	Information Asset Type	Threat	Vulnerability	Source	Security Concern	SOX	PCI	FTC	Probability	Impact	Risk Areas: Financial	Operations	Legal/ Regulatory	Member Loyalty	Initial Risk	Chance of Detection/ Prevention	Risk Priority Number	Risk Rating	Controls	Residual Risk Rating	Risk Disposition	Action Plan	Due Date
		Information, Hardware, Software, Physical Assets, People, Services				C = Conf I = Integrity A = Avail				L: = 0.1 M: = 0.5 H: = 1.0	L = 10 M = 50 H = 100					Prob X Imp L = 0-10 M = 25, 50 H = 100	Very easy = 1 Relatively easy = 2 Effort needed = 3 Low likelihood = 4 Very difficult = 5	Risk X Chance of Detection	L: = 0 - 49 M: = 50-199 H: = 200 - 500	Controls to mitigate/reduce risk	Final risk rating after controls		Initial suggested Action Plan (revise as plan further develops)	
1	1	Information (Member Data)	Unauthorized access leading to theft and/or loss.	1) Unclear access control processes/procedures. 2) Access control process/procedure not followed or is circumvented. 3) Terminated/inactive users are not identified and disabled/removed. 4) Improper access control (user access) review. 5) Ineffective monitoring of account creation/modification.	Quarterly account review. Assessment of system monitoring configurations.	C, I	x	x	x	1.0	100	x	x	x	x	100	4	400	High		High	Reduce		1/31/2013
2	12	Software	Exploit of any of the high number of vulnerabilities can put the company's business operations at risk.	High number of vulnerabilities, particularly critical and exploitable vulnerabilities, on systems in the PCI environment.	Vulnerability trends and stats from vulnerability scan reports.	C, I, A	x	x	x	1.0	100.0		x			100	3	300	High		High	Mitigate		3/31/2013
3	17	Services	Loss of services due to system changes occurring in production without first having been tested in development.	Stage, QA and Dev environments are used for testing of key elements, but not all changes are tested in these environments first.	Sev 1 Incident Reporting	C, I, A	x	x		1.0	100		x			100	2	200	High	Project underway to improve testing environments as part of the Infrastructure Stabilization project.	High	Reduce		12/28/2012
4	18	Services	Introduction of compatibility issues and unresolvable security vulnerabilities which can be exploited putting the infrastructure at risk of service interruptions and	Running operating systems and firmware in the environment (RHEL 4, Cisco) which have reached EOL, are no longer maintained or supported by the vendor, can no longer be patched, and are causing integration issues.	Continuous vulnerability scanning	A	x	x		1.0	100		x			100	1	200	High		High	Mitigate		3/31/2013
5	14	People	Well crafted phishing attacks can potentially result in loss of sensitive information and compromise of user authentication credentials.	Unsuspecting users reveal sensitive information and their userIDs/passwords to an attacker.	Annual User Testing of Policy Control regarding Phishing Attacks. On-going testing shows that employees still fall for phishing schemes.	C, I, A	x	x		1.0	50		x		x	50	4	200	High	Started implementing phishing tests to train and educate users.	High	Reduce		12/31/2012
6	5	Information (Member Data)	Unauthorized access leading to theft and/or loss.	Weaknesses in access control to systems and ineffective monitoring.	Number of findings from default accounts on systems found in vulnerability scans to system configuration settings to events captured in monitoring tools.	C, I	x	x	x	1.0	50	x	x	x	x	50	4	200	High		High	Mitigate		1/31/2013
7	16	People	Breach of security (social engineering, physical security breach) resulting in theft of member data	Lack of security awareness	Employees are continuing to loose LL equipment (laptops) and fall for phishing attacks.	C	x	x	x	0.5	50	x	x	x	x	100	4	400	High	New security training program.	Medium	Reduce		12/31/2012
8	9	Hardware	Hardware/systems Outage - INT	Inefficient incident response causing excessive delay in restoration, no defined Service Level Agreements, outdated BCP, and lacking DRP and IR plans. No annual testing of plans.	Service outage due to firmware upgrade and response time length before services restored.	A	x	x		1.0	100.0	x	x	x	x	100	2	200	High	Issue pertains to P&T Operations and can impact business services - not directly related to information security or PCI.	Medium	Reduce		4/30/2013
9	10	Software	Exploit poorly configured systems exposed to the internet could result in an intruder gaining access to networks and systems.	Incorrect Security configuration setting allows directory traversal in an externally facing web application such that when exploited it can reveal highly sensitive information giving an attacker information they can use to penetrate and further exploit the network.	Annual Pen Test	C, I, A	x			1.0	100		x			100	2	200	High		Medium	Mitigate		12/21/2012
10	2	Information (Member Data)	Compromise of Administrative level Authentication Credentials giving unauthorized privileged access to systems.	Using unsecure communications protocols which pass authentication credentials in the clear (i.e., unencrypted RDP to Windows 2003 Servers, RSH between NetApp filers, VNC, TFTP).	Continuous vulnerability scanning	C, I		x		0.5	100		x			50	4	200	High		Medium	Reduce		12/28/2012
11	3	Information (Member Data)	Unauthorized access and potential for system compromise and information loss.	Using weak cipher algorithms, weak keys, encryption that has been successfully hacked (i.e., MD5, SSH Protocol version 1, 56-bit encryption, RSA keys with key length of 1024 bits or less), and vendor supplied self-signed certificates.	Continuous vulnerability scanning	C, I		x		0.5	100		x			50	4	200	High		Medium	Reduce		Critical systems - 12/28/2012 All others - 6/30/2013
12	6	Hardware	Hardware not monitored	Weaknesses in security monitoring for performance, capacity and operational incidents. Deficient HW/SW maintenance program.	On-going Infrastructure Stabilization issues. Critical systems operating on unsupported EOL versions of software/firmware.	I A	x	x	x	0.5	100	x	x	x	x	50	3	150	Medium		Medium	Reduce		5/31/2013
13	7	Hardware	Failure of hardware/systems - INT	Weakness in DRP, BCP	Out of date Infrastructure BCP/DRP. Place has not been tested since 2009.	I A	x	x	x	0.5	100	x	x	x	x	50	3	150	Medium		Medium	Reduce		5/30/2013
14	13	Physical Assets	Assets used to support member operations are not identified or recorded	Lack of controls to ensure diligence in performing asset inventory	Out of date and incomplete asset inventory.	I	x	x		1.0	50	x		x		50	3	150	Medium		Medium	Mitigate		2/28/2013
15	8	Hardware	Unauthorized or sabotaged changes to hardware	Lack of standard configurations and build lists for critical components; Lack of proper change control, approvals Weaknesses in file integrity monitoring	Missing configuration standards for system components. Changes circumventing change control management procedure. Weaknesses in FIM.	C I A	x	x	x	0.5	50	x	x	x		25	3	75	Medium		Medium	Reduce		3/31/2013
16	15	People	Unauthorized access to member data terminated employees or employees changing positions	Weaknesses in employee termination process	Accounts of terminated employees still active on systems.	C	x	x	x	0.5	50		x	x	x	25	3	75	Medium		Medium	Reduce		2/28/2013
17	11	Software	"Hackers" (external or internal) attempt to exploit possible system vulnerabilities to gain access to member data or crash systems.	Lack of 24/7 network and security monitoring staff to respond to hacker attempts.	Observation	C, A	x			0.5	50	x	x	x	x	25	2	50	Medium	Implemented Alert Logic early December.	Low	Reduce		4/30/2013
18	4	Information (Member Data)	Loss, theft, tampering or disclosure of member sensitive data by 3rd Party service provider and vendors.	Weakness in Vendor Management processes.	Annual review of vendor list showing it is not up to date with current list of vendors.	C, I	x	x		0.1	100.0		x			10	4	40	Low		Low	Reduce		4/30/2013

“HIGH RPN 2012” worksheet

	Risk ID #	Information Asset Type	Threat	Vulnerability	Source	Security Concern	SOX	PCI	FTC	Probability	Impact	Risk Areas				Initial Risk	Chance of detection	Risk Priority Number	Risk Rating	Controls	Residual Risk Rating	Risk Disposition	Action Plan	Due Date	Notes/Reference
		Information, Hardware, Software, Physical Assets, People, Services				C = Conf I = Integrity A = Avail				L: = 0.1 M: = 0.5 H: = 1.0	L: = 10 M: = 50 H: = 100	Financial	Operations	Legal/ Regulatory	Member Loyalty	Prob X Imp L = 0-10 M = 25, 50 H = 100	Very easy = 1 Relatively easy = 2 Effort needed = 3 Low likelihood = 4 Very difficult = 5	Risk X Chance of Detection	L: = 0 - 49 M: = 50-199 H: = 200 - 500	Controls to mitigate/reduce risk	Final risk rating after controls		Initial suggested Action Plan (revise as plan further develops)		
1	1	Information (Member Data)	Unauthorized access leading to theft and/or loss.	1) Unclear access control processes/procedures. 2) Access control process/procedure not followed or is circumvented. 3) Terminated/inactive users are not identified and disabled/removed. 4) Improper access control (user access) review. 5) Ineffective monitoring of account creation/modification.	Quarterly account review. Assessment of system monitoring configuratoins.	C, I	x	x	x	1.0	100	x	x	x	x	100	4	400	High		High	Reduce		1/31/2013	
2	12	Software	Exploit of any of the high number of vulnerabilites can put the company's business operations at risk.	High number of vulnerabilities, particularly critical and exploitable vulnerabilities, on systems in the PCI environmnet.	Vulnerability trends and stats from vulnerability scan reports.	C, I, A	x	x	x	1.0	100.0		x			100	3	300	High		High	Mitigate		3/31/2013	
3	17	Services	Loss of services due to system changes occurring in production without first having been tested in development.	Stage, QA and Dev environments are used for testing of key elements, but not all changes are tested in these environments first.	Sev 1 Incident Reporting	C, I, A	x	x		1.0	100		x			100	2	200	High	Project underway to improve testing environments as part of the Infrastructure Stabilization project.	High	Reduce		12/28/2012	
4	18	Services	Introduction of compatibility issues and unresolvable security vulnerabilities which can be exploited putting the infrastructure at risk of service interruptions and various possible compromises.	Running operating systems and firmware in the environment (RHEL 4, Cisco) which have reached EOL, are no longer maintained or supported by the vendor, can no longer be patched, and are causing integration issues.	Continuous vulnerability scanning	A	x	x		1.0	100		x			100	1	200	High		High	Mitigate		3/31/2013	
5	14	People	Well crafted phishing attacks can potentially result in loss of sensitive information and compromise of user authentication credentials.	Unsuspecting users reveal sensitive information and their userIDs/passwords to an attacker.	Annual User Testing of Policy Control regarding Phishing Attacks. On-going testing shows that employees still fall for phishing schemes.	C, I, A	x	x		1.0	50		x		x	50	4	200	High	Started implementing phishing tests to train and educate users.	High	Reduce		12/31/2012	
6	5	Information (Member Data)	Unauthorized access leading to theft and/or loss.	Weaknesses in access control to systems and ineffective monitoring.	Number of findings from default accounts on systems found in vulnerability scans to system configuration settings to events captured in monitoring tools.	C, I	x	x	x	1.0	50	x	x	x	x	50	4	200	High		High	Mitigate		1/31/2013	

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __70__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document.**

GT GreenbergTraurig

CONFIDENTIAL

Andrew G. Berg
Tel 202.331.3181
Fax 202.331.3101
berga@gtlaw.com

October 22, 2014

Gregory Madden, Esq.
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mailcode: CC-9528
Washington, DC 20580

Re: LifeLock, Inc.

Dear Mr. Madden:

This responds to your October 10th letter setting forth follow-up requests relating to LifeLock's information and data security practices as well as certain of its alerting practices. We have set forth the requested information following the order of the requests in your letter. (Please note that your questions are set forth below in bold typeface.)

1. Monitoring Activities

a. **Monitoring Procedures Created. In LifeLock's response to the FTC's September 2, 2014 request LifeLock stated that the "Monitoring Procedures" identified in Bates Number LIFELOCK-0023355-358 were "created" in September 2012. LifeLock – 0110777. Please provide the precise date the Monitoring Procedures were created and identify any documents related to the creation of those Monitoring Procedures.**

Produce all documents supporting your response. If you believe these documents were produced previously, please identify them by Bates Number.

The precise date the Monitoring Procedures identified in Bates Number LIFELOCK-0023355-358 were created was September 3, 2012. After a reasonable investigation, we have located no additional documents related to the creation of these Monitoring Procedures.

b. **Specific Reports**

i. For each of the below listed alerts or reports: (a) identify each date that LifeLock received each such report or alert from the date the Monitoring Procedures were first created; (b) explain their purpose and function; and (c) describe the process for tracking and handling:

- **each category of** (b)(3);6(f), (b)(4) **alert (e.g. Tumbleweed Brute Force);**
- (b)(3);6(f),(b)(4) **alerts;**

(b)(3):6(f),(b)(4)

(3) If LifeLock cannot determine whether any company information was accessed, state whether there is any indication that company information was made available to any third party.

(b)(3):6(f),(b)(4)

(4) Describe how each compromised credential was used from the point it was first compromised until the point that the compromise was eliminated.

(b)(3):6(f),(b)(4)

Produce all documents relating to this incident. If you believe these documents were produced previously, please identify them by Bates Number:

(b)(3):6(f),(b)(4)

3. Risk Assessment References

In its April 15, 2014 response, LifeLock explained it conducted "two internal information security risk assessments since October 2013." LIFELOCK – 3171. Please identify, by Bates Number, these two risk assessments.

These risk assessment documents were produced with LifeLock's April 5, 2014 response as Bates Numbers LIFELOCK-0075439 and LIFELOCK-0079743 to 0079744.

4. Delayed Alerts Notifications

LifeLock has previously identified instances of delayed alerts (e.g., for planned maintenance, (b)(3):6(f),(b)(4) . Please identify each instance of delayed alert where LifeLock notified its customers that LifeLock's alert would be, or may have been,

Please accord the foregoing information and enclosed materials confidential treatment under the Commission's Rules of Practice.

Very truly yours,

Andrew Berg H.B.

Andrew G. Berg
Counsel to LifeLock, Inc.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __71__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains excerpted pages only and does not contain all of the pages in the full bates range of the original document. This Exhibit also contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

Results and Recommendations

(b)(3):6(f),(b)(4) identified the following findings to support the conclusion that the user's thin client session on REDACT was infected with Cryptowall. The infection was a result of a Flash based browser redirection attack made possible by an outdated version of Adobe Flash Player.

Finding	Description
Web redirection captured in Palo Alto log file.	The traffic capture indicates the user was unknowingly redirected to a malicious website where a flash based exploit was used to download and execute Cryptowall malware.
The installed version of Adobe Flash Player is vulnerable to attack.	The Flash redirection attack only works on versions of Adobe Flash Player previous to 13.0.0.206. Adobe Flash Player version 12.0.0.4 is installed on REDAC and is vulnerable to this attack.
The installed version of Java was discovered to be out of date and vulnerable to attack.	Although not responsible for the vulnerability exploited during this attack, Java is out dated and should be updated to the current version.
No indication of data exfiltration.	Based on the examination of evidence, there is no indication data was exfiltrated from REDA.

Table 7: Findings

Based on the results of the investigation, (b)(3):6(f),(b)(4) has provided the following recommendations to DLA's client. These recommendations are made to provide DLA a response to this investigation and to better support investigations in the future.

Finding	Recommendation	Priority
Adobe Flash Player is out of date and is vulnerable to attack.	[redacted]	
Java is out of date and is vulnerable to attack.		
Multiple applications were out of date on the local endpoint.		
Cryptolocker was executed from the users AppData directory.		

Table 8: Recommendations

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. LifeLock, Inc., *et al*, Defendants.	**No. CV-10-00530-PHX-MHM** **FEDERAL TRADE COMMISSION'S MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LODGED UNDER SEAL

FTC PROPOSED EXHIBIT __73__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.

***This Exhibit contains redactions which are identified in the document by blacked out text or the text "REDACTED."**

DECLARATION OF VINAYAK BALASUBRAMANIAN PURSUANT TO 28 U.S.C. § 1746

I, VINAYAK BALASUBRAMANIAN, hereby declare as follows:

1. My name is Vinayak Balasubramanian. I am a citizen of the United States and am over eighteen years of age. Unless stated otherwise, I have personal knowledge of the facts contained in this Declaration. If called as a witness, I could and would testify to the facts stated herein.

2. I am an Honors Paralegal with the Federal Trade Commission ("FTC"), in the Bureau of Consumer Protection. I have been an employee of the FTC since August 2014. My duties include conducting consumer interviews and analyzing company documents related to FTC investigations and projects, as well as supporting FTC attorneys in litigation.

3. I received a bachelor's degree with honors in economics from the University of North Carolina at Chapel Hill in May 2014.

4. I was assigned to the FTC's investigation of LifeLock, Inc. ("LifeLock"). As part of my assignment, I was asked by counsel to prepare several spreadsheets and analyze data from various documents that LifeLock provided to the FTC.

Creating 'IP Addresses.xlsx'

5. FTC counsel ask me to prepare a spreadsheet of the IP addresses in the documents identified to me as the list of IP addresses in the 2013 PCI assessment (LIFELOCK-0016188, attached hereto as Exhibit A) ("PCI Assessor List"), spreadsheet created by Gwen Ceylon in January 2013 (LIFELOCK-085250, located at Exhibit 47A of

the FTC's Memorandum in Support of Its Motion for Contempt Against LifeLock, Inc. ("FTC Memorandum")) ("Ceylon List"), LifeLock's log of an internal scan run in January 2013 (LIFELOCK-009622, attached hereto as Exhibit B), and LifeLock's list of decommissioned servers (LIFELOCK-0138076, located at Attachment 32 of the Expert Report of Dr. Eric B. Cole ("Cole Report")) ("Decommissioned List"). These documents contained different but overlapping lists of IP addresses. FTC counsel requested that the spreadsheet enable identification of the overlapping IP addresses. The spreadsheet that I created is entitled 'IP Address.xlsx' and is attached hereto as Exhibit C.

6. I manually inputted the number codes associated with the IP addresses, the computer names, IP addresses, and the descriptions of the IP addresses from the PCI Assessor's List into 'IP Address.xlsx.' This information is in the spreadsheet's columns A, B, D, and F, respectively.

7. I used the Match function in Excel to identify the IP addresses in the Ceylon and Internal Scan Lists that are not in the PCI Assessor's List and added these to the spreadsheet's column B.

8. The Ceylon List identified the operating system and number of vulnerabilities for each IP address listed. I took this information and added it to the spreadsheet's columns H and I, respectively.

9. The Internal Scan List identified the computer name, operating system, number of exploits, number of malware, number of vulnerabilities, risk ranking, and status for each IP address listed. I added this information into the spreadsheet's columns L through R, respectively.

10. I created a separate worksheet labeled 'Decommissioned' in the same spreadsheet and inputted the names of the decommissioned servers from the Decommissioned List.

11. I then compared the information inputted into the spreadsheet from the 4 lists. I used Excel's Match function to compare the IP addresses in each of the 4 lists with the list of all of the IP addresses in the spreadsheet. In columns C, G, K, and S, I indicated whether the specific IP addresses in column B are in these lists.

12. I used Excel's Match function to compare the machine name for each IP address in the Assessor's List with the machine name in the Internal Scan List. Column E states whether the computer names from the two lists match. If the only discrepancy between the machine names was the lack of a domain, I wrote "NO (missing domain)" in the column. If the computer name was not available in both lists, I wrote "N/A."

13. I used Excel's Match function to compare the number of vulnerabilities identified for each IP address in the Ceylon List and the Internal Scan List. Column J states whether the two lists identified the same number of vulnerabilities for each IP address. If the number of vulnerabilities was not available in both lists, I wrote "N/A."

Creating 'Microsoft Patches.xlsx'

14. FTC counsel asked me to prepare a spreadsheet calculating the number of days between the release of each Microsoft security bulletin and the installation of the corresponding patches on each computer identified in 'LIFELOCK-0136812.csv' located in Attachment 29 of the Cole Report. The completed spreadsheet 'Microsoft Patches.xlsx' is attached hereto as Exhibit D.

15. 'LIFELOCK-0136812.csv' contained one row for each combination of computer IDs and Hot Fix IDs. Each Hot Fix ID contained at least one CVE number, and most of the data contained multiple CVE numbers in the same row. FTC counsel informed me that each CVE is associated with a unique Microsoft patch. I created the worksheet 'Hotfix-CVE Data' to reorganize the data so that each row contains a distinct combination of computer IDs, Hot Fix IDs, and CVE numbers. Since most identical Hot Fix IDs throughout the data were associated with the same set of CVE numbers, I prepared a table for each distinct Hot Fix ID and set of CVE numbers, and used the Excel functions for separating the set of CVE numbers into columns and transposing data to enable that each row contained a distinct Hot Fix ID and CVE number.

16. I incorporated the Microsoft publish date, bulletin ID number, and criticality level for each entry in the worksheet 'Hotfix-CVE Data' by using the following methodology:

    a. I determined the publish date of each Hot Fix ID number by visiting support.microsoft.com.

    b. I determined the bulletin ID number for each CVE by visiting the webpage for the security bulletins that were installed during the month of the publish date, and reviewing the Exploitability Index table for the CVEs, and determining their corresponding bulletin IDs.

    c. I determined the criticality for all CVEs in each bulletin ID by reviewing the executive summaries table.

17. In some instances, information on support.microsoft.com showed that some of the CVE numbers were not associated with the Hot Fix ID number identified by 'LIFELOCK-0136812.csv.' For these CVE numbers, I used the publish date for the Hot Fix ID number and manually researched the bulletin ID and criticality for the respective CVE numbers. I marked each data point that was determined using this method under column F.

18. I checked to see if there were any matches between the computer names listed in the spreadsheet and the computer names that were located in 'IP Address.xlsx.' To do this, I created the worksheet 'IP Address Data.' I modified the computer names identified in 'LIFELOCK-0136812.csv' so that the name only has the portion of the name before the first period (.) and used Excel's Match function to determine if any computer name was on either the PCI Assessor List or the Internal Scan List. For the ones that were on either list, I noted the IP addresses. I then used Excel to copy the noted IP addresses into the worksheet 'IP Address Data' in the rows with their respective computer names.

19. I merged the 'Hotfix-CVE Data' and 'IP Address Data' worksheets to create the worksheet 'Data Merge1.' I was able to automate the process for data points with only one CVE number, as I used Excel's Match function to match and merge the two datasets accordingly. I had to manually do this for data points with multiple CVE numbers. I copied all of these data points and pasted them into a new worksheet, called 'Data Merge 2.' I pasted it as many times as there were CVE

numbers. Then, I was able to copy each CVE number (and its corresponding publish date, bulletin ID, and criticality) into each set of pasted data.

20. I copied the data in 'Data Merge1' and 'Data Merge 2' to a new worksheet entitled 'Microsoft Patches' and used Excel's DAYS360 function in column S to compute the number of days between the publish date in column L with the install date in column D.

21. At the request of FTC counsel, I also added the worksheet 'Select Patches.' This worksheet analyzes whether 17 critical Microsoft operating system patches were applied to the 17 IP addresses that were identified in 'LIFELOCK-0136812.csv,' included in both Ceylon's List and the PCI Assessor List, and identified as "Windows" in Ceylon's List. The 17 critical patches were identified to me by counsel, and I entered them as separate columns. I identified 17 IP addresses meeting the above criteria by using Excel's Filter function in the 'IP Addresses.xlsx' spreadsheet and entered each of these as a separate row in the 'Select Patches' worksheet. I determined whether these 17 IP addresses received each of the 17 critical patches by using Excel's Sort & Filter functions and noted that determination in the columns labeled "Installed?" by typing 'X' to indicate a patch installation for the IP address. For the IP addresses that received a patch, I obtained the patch installation date and the Installation Time from worksheet 'Microsoft Patches' and noted the same manually in the columns labeled "Install Date" and "Days since Published." In some instances for one of the patches, the "Days since Published" data in the 'Select Patches' worksheet was different from

the respective data point in the 'Microsoft Patches' worksheet since the publish date in the 'Select Patches' referred to the Microsoft patch, while the publish date in the 'Microsoft Patches' spreadsheet referred to the Hot Fix ID. This discrepancy was limited to the data identified in Paragraph 17 above. For each critical patch, I used Excel's Average function to calculate the average Installation Time for all IP addresses that received the patch and the total number of IP addresses that received the patch. For each IP address, I manually counted the total number of critical patches installed in column BA, manually entered the date ranges for installation of the critical patches for the IP address in column BB, and used Excel's Average function to calculate the average Installation Time for all critical patches that were installed on the IP address in column BC.

22. FTC counsel asked me to create a new worksheet – 'Microsoft Patch with LL Ratings' – that included LifeLock's criticality ratings (the column entitled "LifeLock Severity") that were located in the file 'workingLIFELOCK-0138080.xlsx'.[1] To do this, I looked at the HotFix Bulletin ID and LifeLock Severity columns and eliminated duplicates. I found that, while most Hot Fixes had been assigned the same LifeLock criticality rating throughout the data, there were some that had been assigned multiple ratings that appeared to vary by server. I used the SORT function to quickly copy the Hot Fix ID and LifeLock Severity data where the Hot Fix ID had been assigned the same rating for all servers. For

[1] I compared 'workingLIFELOCK-0138080.xlsx' with 'LIFELOCK-0138080.csv' in Attachment 29 of the Cole Report using the 'Match' function in Excel and found that the data in the two files were identical.

the Hot Fix ID numbers that were assigned more than one rating, I used the SORT and FILTER functions to manually copy each rating into its server.

Creating 'Linux Patches.xlsx'

23. FTC counsel asked me to prepare a spreadsheet calculating the number of days between the release of each Red Hat Security Advisory (RHSA) and the installation of the corresponding patches on each computer identified in 'LIFELOCK-0136813.csv' (Attachment 29 of the Cole Report). The completed spreadsheet 'Linux Patches.xlsx' is attached hereto as Exhibit E.

24. 'LIFELOCK-0136813.csv' contained one row for each combination of server names and RHSA numbers. I used Excel's 'Remove Duplicates' function to remove duplicate RHSAs and identified 18 unique RHSAs in 'LIFELOCK-0136813.csv.' I listed these 18 unique RHSAs in a new spreadsheet 'Linux Patches.xlsx' in the worksheet 'RHSA Data.'

25. I looked up the webpages containing information regarding these 18 RHSAs on rhn.redhat.com and entered the issue date and criticality level for each RHSA into columns B and C in the worksheet 'RHSA Data.'

26. I checked to see if there were any matches between the computer names listed in the 'Linux Patches' worksheet and the computer names that were located in 'IP Address.xlsx.' To do this, I created the worksheet 'IP Address Data.' I modified the computer names identified in 'Linux Patches' worksheet so that the name only has the portion of the name before the first period (.) and used Excel's Match function to determine if any computer name was on either the PCI Assessor List or

the Internal Scan List. For the ones that were on either list, I noted the IP addresses. I then used Excel to copy the noted IP addresses into the worksheet 'IP Address Data' in the rows with their respective computer names.

27. I merged the 'RHSA Data' and 'IP Address Data' worksheets using Excel's Match function to create the worksheet 'Linux Patches.' I manually re-entered the installation dates in column D of 'Linux Patches' into "month/day/year" format in column E so that Excel could recognize the dates. I used Excel's DAYS360 function in column N to calculate the number of days between the date of release of the RHSA in column K and the date of installation of the corresponding patches in column E.

28. FTC counsel later asked me to merge LifeLock's criticality ratings (the column entitled "LifeLock Severity") that were located in the file 'workingLIFELOCK-0138079.xlsx.'[2] To do this, I looked at the RHSA and LifeLock Severity columns and eliminated duplicates. I found that, while most Hot Fixes had been assigned the same LifeLock criticality rating throughout the data, there were some that had been assigned multiple ratings that appeared to vary by server. I used the SORT function to quickly copy the RHSA and LifeLock Severity data where the RHSA had been assigned the same rating for all servers. For the RHSA numbers that were assigned more than one rating, I used the SORT and FILTER functions to

[2] I compared the file 'workingLIFELOCK-0138079.xlsx' with 'LIFELOCK-0138079.csv' in Attachment 29 of the Cole Report using the 'Match' function in Excel and found that the data in the two files were identical.

manually copy each rating into its server. The criticality rating column for LifeLock is included in column M of the 'Linux Patches' worksheet.

29. In the process of merging data, I noticed that there were multiple entries for many data points containing the same server name, RHSA, and install dates. The numerous duplicates appeared to be caused by miscellaneous entries in the "Update Package" column, as well as minor variations in the time of day that these miscellaneous "update packages" were installed. FTC counsel instructed me to delete these additional entries. To do so, I created a new worksheet entitled "Linux Patches (no duplicates)' and deleted the column containing the precise date and time, as well as the 'update package.' After deleting these columns, I used the 'Remove Duplicates' function to eliminate the additional entries.

30. FTC counsel instructed me to prepare a version of the Linux spreadsheet where each data point was a separate CVE number. Since each RHSA number was associated with the same set of CVE numbers, and since there was a limited number of distinct RHSA numbers, I was able to manually complete this process. I copied all of these data points and pasted them into a new worksheet, called 'Linux Patches – By CVE.' I pasted it as many times as there were CVE numbers. Then, I was able to copy each CVE number (and its corresponding publish date, bulletin ID, Linux criticality, and LifeLock criticality) into each set of pasted data.

Creating 'Data Analysis.docx'

31. FTC counsel asked me to identify the IP addresses that are identified as Linux in the Ceylon List by Gwenn and are on the PCI Assessor List, and to determine

which of these IP addresses received a patch. I used Excel's 'Match' function to make this determination (by matching the IP addresses between the two spreadsheets) and prepared two lists: one of IP Addresses and Machine Names with a patch, and one without any. These two lists are on the first page of the 'Data Analysis.docx.' The completed document "Data Analysis.docx" is attached hereto as Exhibit F.

32. FTC counsel also asked me to prepare a summary of the data in the spreadsheets 'Microsoft Patches.xlsx' and 'Linux Patches.xlsx', specifically analyzing the number of days between the release date of the patch (date of Microsoft HotFix ID or RHSA) and the date of application of the patch ("Installation Time"). For the Linux, I was asked by FTC counsel to prepare separate tables for the 'Linux Patches' worksheet, the 'Linux Patches (no duplicates)' worksheet, and the 'Linux Patches by CVE (no dupl)' worksheet. In the tables entitled 'Microsoft Patch Spreadsheet – Summary Statistics,' 'Linux Patches – Summary Statistics,' 'Linux Patches by CVE (no dupl) – Summary Statistics,' 'Linux Patches (no duplicates) – Summary Statistics,' ' I calculated the total number of patches applied, the mean Installation Time, the standard deviation for Installation Time, lowest Installation Time, 25th percentile Installation Time, median Installation Time, 75th percentile Installation Time, and the highest Installation Time. I also calculated the number and percentage of patches with Installation Time greater than 30 days, 60 days, and 90 days. For all of the worksheets except for the 'Linux Patches' worksheet, I prepared two tables for each of the above sets of summary statistics using each of

the foregoing calculations. The first table included the calculations for each criticality level as defined by Microsoft or Linux (Critical, Important, and Moderate for Microsoft patches; Important, Moderate, and Low for Linux patches), and the second table included the calculations for each criticality level as defined by LifeLock (Critical, Important, 'Med' or Moderate, and Low for Microsoft patches, and Important, Moderate, and Low for Linux patches). I determined all of these data points by using Excel formulas or manual computations. These tables are located on pages 2-6 of 'Data Analysis.docx.'

Creating 'Data Analysis 2.docx'

33. FTC counsel asked me to identify the IP addresses that are identified as Microsoft in the Ceylon List by Gwenn and are on the PCI Assessor List, and to determine which of these IP addresses received a patch. I used Excel's Match function to make this determination (by matching the IP addresses between the two spreadsheets) and prepared two lists: one of IP Addresses and Machine Names with a patch, and one without any. These two lists are on the second and third pages of the 'Data Analysis 2.docx.' The completed spreadsheet 'Data Analysis 2.docx' is attached hereto as Exhibit G.

34. I was also asked by counsel to prepared summary statistics for the Microsoft and Linux patch spreadsheets based on the date that the patch was published. I isolated the Microsoft data from the 'Microsoft Patches' and the Linux data from the 'Linux Patches' worksheet, the 'Linux Patches (no duplicates)' worksheet, and the 'Linux Patches by CVE (no dupl)' worksheets' into three publish periods and

analyzed the average and median number of days between the publish date and install date. I determined these data points by using Excel formulas. For each data period, I also analyzed the average and median number of days for the patches with the highest rating in the dataset as identified by Microsoft and Linux ("Critical" for Microsoft, "Important" for Linux), and as identified by LifeLock ("Critical" for Microsoft, "Important" for Linux) by using the Excel Filter function to restrict the patch data accordingly. I did not analyze the LifeLock criticality data for the 'Linux Patches' worksheet.

35. FTC counsel also asked me to prepare summary statistics for the patch spreadsheets based on the date that the patch was installed. I isolated the Microsoft data from the 'Microsoft Patches' and the Linux data from the 'Linux Patches' worksheet, the 'Linux Patches (no duplicates)' worksheet, and the 'Linux Patches by CVE (no dupl)' worksheets' into three publish periods and analyzed the average and median number of days between the publish date and install date. I determined these data points by using Excel formulas. For each data period, I also analyzed the average and median number of days for the patches with the highest rating in the dataset as identified by Microsoft and Linux ("Critical" for Microsoft, "Important" for Linux), and as identified by LifeLock ("Critical" for Microsoft, "Important" for Linux) by using the Excel Filter function to restrict the patch data accordingly. I did not analyze the LifeLock criticality data for the 'Linux Patches' worksheet.

Creating 'Data Analysis - PCI.docx'

36. FTC counsel asked me to run the same analysis described in Paragraph 32 but for just those machines in 'Microsoft Patches.xlsx' and 'Linux Patches.xlsx' that are also identified in the PCI Assessor List. I used Excel's Filter function to identify the IP addresses in the 'IP Addresses.xlsx' spreadsheet that were identified on the PCI Assessor's List and used Excel's Filter function to limit the data both the Microsoft and Linux Patches to only include these IP addresses. For the Linux, I was asked by FTC counsel to prepare separate tables for the 'Linux Patches' worksheet, the 'Linux Patches (no duplicates)' worksheet, and the 'Linux Patches by CVE (no dupl)' worksheet. In the tables entitled 'Microsoft Patch Spreadsheet (PCI IP Addresses Only) – Summary Statistics,' 'Linux Patch Spreadsheet (PCI IP Addresses Only) – Summary Statistics,' 'Linux Patches by CVE (no dupl) – Summary Statistics,' and 'Linux Patches (no duplicates) (PCI IP Addresses Only) – Summary Statistics,' I calculated the total number of patches applied, the mean Installation Time, the standard deviation for Installation Time, lowest Installation Time, 25th percentile Installation Time, median Installation Time, 75th percentile Installation Time, and the highest Installation Time. I also calculated the number and percentage of patches with Installation Time greater than 30 days, 60 days, and 90 days. For all of the worksheets except for the 'Linux Patches' worksheet, I prepared two tables for each of the above sets of summary statistics using each of the foregoing calculations. The first table included the calculations for each criticality level as defined by Microsoft or Linux (Critical, Important, and

Moderate for Microsoft patches; Important, Moderate, and Low for Linux patches), and the second table included the calculations for each criticality level as defined by LifeLock (Critical, Important, 'Med' or Moderate, and Low for Microsoft patches, and Important, Moderate, and Low for Linux patches). I determined all of these data points by using Excel formulas or manual computations. The completed spreadsheet 'Data Analysis- PCI.docx' is attached hereto as Exhibit H.

37. FTC counsel also asked me to run the same analysis described in Paragraph 34 but for just those machines in 'Microsoft Patches.xlsx' and 'Linux Patches.xlsx' that are also identified in the PCI Assessor List. I used Excel's Filter function to focus on only IP Addresses listed on the PCI Assessor's List, and to isolate the Microsoft data from the 'Microsoft Patches' and the Linux data from the 'Linux Patches' worksheet, the 'Linux Patches (no duplicates)' worksheet, and the 'Linux Patches by CVE (no dupl)' worksheets into three publish periods and analyzed the average and median number of days between the publish date and install date. I determined these data points by using Excel formulas. For each data period, I also analyzed the average and median number of days for the patches with the highest rating in the dataset as identified by Microsoft and Linux ("Critical" for Microsoft, "Important" for Linux), and as identified by LifeLock ("Critical" for Microsoft, "Important" for Linux) by using the Excel Filter function to restrict the patch data accordingly. I did not analyze the LifeLock criticality data for the 'Linux Patches' worksheet.

38. FTC counsel also asked me to run the same analysis described in Paragraph 35 but for just those machines in 'Microsoft Patches.xlsx' and 'Linux Patches.xlsx' that are also identified in the PCI Assessor List. I used Excel's Filter function to focus on only IP Addresses listed on the PCI Assessor's List, and to isolate the Microsoft data from the 'Microsoft Patches' and the Linux data from the 'Linux Patches' worksheet, the 'Linux Patches (no duplicates)' worksheet, and the 'Linux Patches by CVE (no dupl)' worksheets into three install periods and analyzed the average and median number of days between the publish date and install date. I determined these data points by using Excel formulas. For each data period, I also analyzed the average and median number of days for the patches with the highest rating in the dataset as identified by Microsoft and Linux ("Critical" for Microsoft, "Important" for Linux), and as identified by LifeLock ("Critical" for Microsoft, "Important" for Linux) by using the Excel Filter function to restrict the patch data accordingly. I did not analyze the LifeLock criticality data for the 'Linux Patches' worksheet.

Other Tasks

39. FTC counsel asked me to identify the patches that were associated with Vulnerability Request ("VRR") 81561 and were listed in LIFELOCK-0038588-89 (Attachment 11 in the Cole Report). Since the list of patches appeared to be cut off from the document, counsel asked me to review LIFELOCK-0030131-32 (Attachment 12 of the Cole Report), which identifies the Microsoft patches referenced in VRR 81561 and LIFELOCK-0038588-89. My review of

LIFELOCK-0030131-32 showed that there were 20 Microsoft patches identified in VRR 81561. FTC counsel also asked me to review the criticality of each of these patches. I independently reviewed the Microsoft bulletins associated with these patches on www.technet.microsoft.com and determined that fourteen of them were rated "Critical," six of them were rated "Important," and that none of them ranked less than "Important."

40. FTC counsel asked me to compare the identification of the servers with the most vulnerabilities on LIFELOCK-0085250 (Exhibit 47A of the FTC Memorandum) with the list of decommissioned servers that appear on LIFELOCK-0138076 (Attachment 32 of the Cole Report). The nine servers appearing on LIFELOCK-0085250 that have the most vulnerabilities on also appear on the list of decommissioned servers on LIFELOCK-0138076.

41. FTC counsel asked me to take a screenshot of the webpage https://lifelock.custhelp.com/app/answers/detail/a_id/149, which describes how a consumer may know that their information is secure with LifeLock. This webpage is accessible from LifeLock's website. I took a screenshot of this page on July 14, 2015. A copy of this screenshot is attached hereto as Exhibit I.

42. FTC counsel asked me to review LIFELOCK-0135515 (Exhibit 5, Annex 2 of the FTC Memorandum) to see how many times certain LifeLock infomercials featuring Montel Williams had aired. Specifically, I was asked to count all of the advertisements located in the worksheets entitled "SEASON," "STOP," and "LIVINGWELL,MONTEL,MONTEL60." These worksheets showed each time an

advertisement ran by air date, air time, show title, station, and market. I found that there were 1,035 separate airings of advertisements in the worksheet entitled "SEASON," 39,433 separate airings of advertisements in the worksheet entitled "STOP," and 9,093 separate airings of advertisements in the worksheet entitled "LIVINGWELL,MONTEL,MONTEL60." I found that there were 49,561 separate airings of advertisements across all three of the aforementioned worksheets.

43. FTC counsel asked me to review the Vulnerability Remediation Request excerpts from LIFELOCK-0138077-78 (Attachment 13 of the Cole Report) and to count the requests that were dated from June 26-28, 2013. I found that there were 83 requests during this time period that were rated as "critical" or "high."

I declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on July 20, 2015

Vinayak Balasubramanian

VINAYAK BALASUBRAMANIAN

EXHIBIT A

LifeLock PCI Environment Diagram

REDACTED

LifeLock PCI Environment Diagram Legend

Approved by: Rich Stebbins, CIO
Patrick Sorcino, Interim Director of Infrastructure
David Bridgman, Sr. Information Security Engineer

Date: 04/30/2013

1	REDACTED	VIP
2	[redacted]	VIP
3	[redacted]	Network Device
4	[redacted]	Network Device
5	[redacted]	VIP
6	[redacted]	Video System
7	[redacted]	Video System
8	[redacted]	Video System
9	[redacted]	Video System
10	[redacted]	SCCM - Patching
11	[redacted]	Video System
12	[redacted]	Video System
13	[redacted]	Video System
14	[redacted]	Video System
15	[redacted]	Video System
16	[redacted]	Video System
17	[redacted]	Video System
18	[redacted]	Video System
19	[redacted]	NetBackup - Backups
20	[redacted]	Network Device
21	[redacted]	Cisco NAC
22	[redacted]	SCCM - Patching
23	[redacted]	Network Device
24	[redacted]	Network Device
25	[redacted]	Citrix
26	[redacted]	Citrix
27	[redacted]	Citrix
28	[redacted]	Citrix
29	[redacted]	Citrix
30	[redacted]	Citrix
31	[redacted]	Citrix
32	[redacted]	Citrix
161	[redacted]	Citrix
162	[redacted]	Citrix
163	[redacted]	Citrix
164	[redacted]	Citrix
165	[redacted]	Citrix
166	[redacted]	Citrix
167	[redacted]	Citrix
168	[redacted]	Citrix
169	[redacted]	Citrix
170	[redacted]	Citrix
171	[redacted]	Citrix
172	[redacted]	Citrix
173	[redacted]	Citrix
174	[redacted]	Citrix
175	[redacted]	Citrix
176	[redacted]	Citrix
34	[redacted]	Informatica - BI Automation
36	[redacted]	Jenkins - Job Automation
37	[redacted]	DB Grid Control Server
38	[redacted]	WSUS - Patching
39	[redacted]	Tumbleweed Data Repository
40	[redacted]	PGP Server - Disk Encryption
41	[redacted]	SCCM - Patching
42	[redacted]	Storage Mgmt Tool
43	[redacted]	Batch Job Automation
44	[redacted]	SCCM - Patching
45	[redacted]	NetBackup - Backups
46	[redacted]	NetBackup - Backups
47	[redacted]	SEP - Antimalware Management

48	REDACTED	(b)(3):6(f),(b)(4)
49	[redacted]	
50	[redacted]	
51	[redacted]	
52	[redacted]	
53	[redacted]	
54	[redacted]	
55	[redacted]	
56	[redacted]	
57	[redacted]	
58	[redacted]	
60	[redacted]	
61	[redacted]	
62	[redacted]	
63	[redacted]	
64	[redacted]	
73	[redacted]	
74	[redacted]	
75	[redacted]	
76	[redacted]	
77	[redacted]	
78	[redacted]	
79	[redacted]	
80	[redacted]	
81	[redacted]	
83	[redacted]	
84	[redacted]	
85	[redacted]	
86	[redacted]	
87	[redacted]	
88	[redacted]	
89	[redacted]	
90	[redacted]	
91	[redacted]	
92	[redacted]	
93	[redacted]	
94	[redacted]	
95	[redacted]	
96	[redacted]	
97	[redacted]	
98	[redacted]	
99	[redacted]	
100	[redacted]	
101	[redacted]	
102	[redacted]	
103	[redacted]	
104	[redacted]	
105	[redacted]	
106	[redacted]	
107	[redacted]	
108	[redacted]	
109	[redacted]	
110	[redacted]	
111	[redacted]	
112	[redacted]	
113	[redacted]	
114	[redacted]	
115	[redacted]	
116	[redacted]	
117	[redacted]	
118	[redacted]	

119	REDACTED	Application Support Jump Box
120	[redacted]	Member Portal Proxy Application
121	[redacted]	Member Portal Proxy Application
122	[redacted]	OSB, Web Logic
123	[redacted]	SQL Server Database
124	[redacted]	SQL Server Database
125	[redacted]	Metranet - VIP
126	[redacted]	Metranet - VIP
127	[redacted]	Metranet - VIP
128	[redacted]	VIP
129	[redacted]	VIP
130	[redacted]	Network Device
131	[redacted]	Network Device
132	[redacted]	Oracle (OLTP) Database
133	[redacted]	Oracle (OLTP) Database
134	[redacted]	Blade Center Consoles
135	[redacted]	Blade Center Consoles
136	[redacted]	Blade Center Consoles
137	[redacted]	Blade Center Consoles
138	[redacted]	Blade Center Consoles
177	[redacted]	Blade Center Consoles
178	[redacted]	Blade Center Consoles
179	[redacted]	Blade Center Consoles
180	[redacted]	Blade Center Consoles
181	[redacted]	Blade Center Consoles
182	[redacted]	Blade Center Consoles
183	[redacted]	Blade Center Consoles
141	[redacted]	Network Device
142	[redacted]	Network Device
143	[redacted]	Network Device
144	[redacted]	Network Device
145	[redacted]	Network Device
146	[redacted]	Network Device
147	[redacted]	Network Device
148	[redacted]	Network Device
149	[redacted]	Network Device
150	[redacted]	Network Device
151	[redacted]	Network Device
152	[redacted]	Network Device
155	[redacted]	Network Device
156	[redacted]	Network Device
157	[redacted]	ACS - Authentication
158	[redacted]	ACS - Authentication
159	[redacted]	Verisign - Two-factor
160	[redacted]	Verisign - Two-factor
184	[redacted]	NetApp Filer - Storage (site2)
185	[redacted]	NetApp Filer - Storage (site2)
186	[redacted]	Verint Enterprise server
187	[redacted]	Variant RSA ClearTrust server
188	[redacted]	Variant Call Recorder
189	[redacted]	Verint recorder manager
190	[redacted]	Variant Database server
191	[redacted]	Variant forecasting and Scheduling
192	[redacted]	Variant Call Survey
193	[redacted]	Sip Router CentryLink MPLS
194	[redacted]	Sip Router TW Telecom
195	[redacted]	Switch Sungard SCT
196	[redacted]	Sip Cube Router
197	[redacted]	Sip Switch
198	[redacted]	TW Telcom MPLS
199	[redacted]	CCX MOE

REDACTED	Infrastructure
[redacted]	Database
[redacted]	Application
[redacted]	Presentation
[redacted]	Storage
[redacted]	Authentication
[redacted]	ESX (Virtual Host)
[redacted]	Logging/Monitoring
[redacted]	Management
[redacted]	Deployment
[redacted]	Citrix
[redacted]	DMZ
[redacted]	Network
[redacted]	Network
[redacted]	Management
[redacted]	Management
[redacted]	Storage

LIFELOCK-0016188

CONFIDENTIAL

FTC-0002893

[redacted]

REDACTED

FTC-0002894

EXHIBIT B

FTC has submitted the document(s) in this Exhibit in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

EXHIBIT C

FTC has submitted the document(s) in this Exhibit in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

EXHIBIT D

FTC has submitted the document(s) in this Exhibit in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

EXHIBIT E

FTC has submitted the document(s) in this Exhibit in native format on CD with its contemporaneously filed Motion for Leave to Allow the Non-Electronic Filing of Exhibits.

EXHIBIT F

Data Analysis

NOTE: There are 34 IP addresses that were identified as Linux by Gwenn and were on the PCI assessor's list. The following 2 IP addresses received at least one patch.

IP Addresses	Machine Name
REDACTED	

The remaining 32 IP addresses did NOT receive any patch, and are listed below.

IP Addresses	Machine Name
REDACTED	

Below are summary statistics for the Microsoft and Linux patch spreadsheets.

Microsoft Patch Spreadsheet – Summary Statistics				
	Importance of Patch (Microsoft Ratings)			
	All	Critical	Important	Moderate
Total Number	4755	2290	2421	44
Percent of Whole	100	48.160	50.915	0.9253
Mean	44.387	59.775	29.478	63.909
St. Dev	57.592	76.963	21.355	16.918
Lowest	0	0	1	31
25th percentile	15	10	15	60
Median	31	35	31	71
75th percentile	49	72	38	72
Highest	667	667	199	90
>30 days (#)	2622	1297	1280	44
>30 days (%)	55.142	56.638	52.871	100
>60 days (#)	884	741	109	36
>60 days (%)	18.591	32.358	4.502	81.818
>90 days (#)	469	403	66	0
>90 days (%)	9.863	17.598	2.726	0

Microsoft Patch Spreadsheet – Summary Statistics					
	Importance of Patch (LifeLock Ratings)				
	All	Critical	Important	Med/Moderate	Low
Total Number	4755	2193	2381	53	128
Percent of Whole	100	46.120	50.074	1.115	2.692
Mean	44.387	58.404	28.972	68.679	80.922
St. Dev	57.592	78.140	20.695	18.533	33.603
Lowest	0	0	1	31	58
25th percentile	15	8	15	63	58
Median	31	33	31	72	58
75th	49	70	38	79	92

percentile					
Highest	667	667	199	92	182
>30 days (#)	2622	1193	1247	53	128
>30 days (%)	55.142	54.400	52.373	100	100
>60 days (#)	884	696	91	43	54
>60 days (%)	18.591	31.737	3.822	81.132	42.188
>90 days (#)	469	359	47	9	54
>90 days (%)	9.863	16.370	1.974	16.981	42.188

'Linux Patches' Worksheet – Summary Statistics				
	Importance of Patch (Linux Ratings)			
	All	**Important**	**Moderate**	**Low**
Total Number	1531	48	749	734
Percent of Whole	100	3.135	48.922	47.943
Mean	147.064	64.813	190.828	107.785
St. Dev	125.318	55.767	99.533	136.191
Lowest	8	23	8	16
25th percentile	29	30	33	29
Median	56	55	234	29
75th percentile	238	59	238	78
Highest	351	196	287	351
>30 days (#)	928	30	596	302
>30 days (%)	60.614	62.5	79.573	41.144
>60 days (#)	755	10	553	192
>60 days (%)	49.314	20.833	73.832	26.158
>90 days (#)	734	7	547	180
>90 days (%)	47.943	14.583	73.031	24.523

'Linux Patches By CVE (no dupl)' Worksheet– Summary Statistics				
	Importance of Patch (Linux Ratings)			
	All	Important	Moderate	Low
Total Number	1540	55	935	551
Percent of Whole	100	3.571	60.714	35.779
Mean	148.839	115.556	159.737	133.608
St. Dev	124.469	72.280	109.235	148.270
Lowest	8	23	8	16
25th percentile	29	55	29	29
Median	78	65	234	29
75th percentile	238	193	238	346
Highest	351	196	287	351
>30 days (#)	950	45	642	263
>30 days (%)	61.688	81.818	68.663	47.731
>60 days (#)	783	31	563	189
>60 days (%)	50.844	56.364	60.214	34.301
>90 days (#)	756	25	551	180
>90 days (%)	49.091	45.455	58.930	32.668

'Linux Patches (no duplicates)' worksheet – Summary Statistics				
	Importance of Patch (Linux Ratings)			
	All	Important	Moderate	Low
Total Number	1141	29	561	551
Percent of Whole	100	2.542	49.167	48.291
Mean	153.787	70.966	177.888	133.608
St. Dev	131.719	57.557	110.401	148.270
Lowest	8	23	8	16
25th percentile	29	30	29	29
Median	56	56	234	29
75th	282	63	282	346

percentile				
Highest	351	196	287	351
>30 days (#)	695	20	412	263
>30 days (%)	60.911	68.966	73.440	47.731
>60 days (#)	566	8	369	189
>60 days (%)	49.606	27.586	65.775	34.301
>90 days (#)	548	5	363	180
>90 days (%)	48.028	17.241	64.706	32.668

'Linux Patches By CVE (no dupl)' Worksheet– Summary Statistics				
	Importance of Patch (LifeLock Ratings)			
	All	**Important**	**Moderate**	**Low**
Total Number	1540	34	933	573
Percent of Whole	100	2.208	60.584	37.208
Mean	148.839	128.529	159.906	132.024
St. Dev	124.469	77.479	109.291	146.035
Lowest	8	23	8	16
25th percentile	29	30	29	29
Median	78	193	234	30
75th percentile	238	193	238	346
Highest	351	193	287	351
>30 days (#)	950	25	640	285
>30 days (%)	61.688	73.529	68.596	49.738
>60 days (#)	783	20	561	202
>60 days (%)	50.844	58.824	60.129	35.253
>90 days (#)	756	20	551	185
>90 days (%)	49.091	58.824	59.057	32.286

'Linux Patches (no duplicates)' worksheet – Summary Statistics				
	Importance of Patch (LifeLock Ratings)			
	All	**Important**	**Moderate**	**Low**
Total Number	1141	18	560	563
Percent of Whole	100	1.578	49.080	49.343
Mean	153.787	71.222	178.061	132.282
St. Dev	131.719	66.032	110.424	147.063
Lowest	8	23	8	16
25th percentile	29	29	29	29
Median	56	31.5	234	29
75th percentile	282	90.25	282	346
Highest	351	193	287	351
>30 days (#)	695	9	411	275
>30 days (%)	60.911	50.000	73.393	48.845
>60 days (#)	566	4	368	194
>60 days (%)	49.606	22.222	65.714	34.458
>90 days (#)	548	4	363	181
>90 days (%)	48.028	22.222	64.821	32.149

EXHIBIT G

Microsoft Patches			
	Date Published		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	1416	2882	457
Average	87.39	29.22	6.81
Median	64.5	31	3
Average - Critical	93.41	31.07	6.80
Median - Critical	67	26	3
Average – Critical (LL)	94.742	30.339	6.805
Median – Critical (LL)	69	22.949	3

Linux Patches			
	Date Published		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	736	791	4
Average	272.39	31.16	8
Median	238	29	8
Average – Important	194.29	42.71	-
Median – Important	193	33	-

Microsoft Patches			
	Date Installed		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	1019	1530	2206

Average	77.59	37.44	33.87
Median	58	17	31
Average - Critical	83.53	56.43	33.26
Median - Critical	58	35	17
Average – Critical (LL)	84.164	55.728	32.368
Median – Critical (LL)	58	35	17

Linux Patches			
	Date Installed		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	2	1446	83
Average	26	151.74	68.49
Median	26	213	56
Average - Important	-	-	64.81
Median - Important	-	-	55

Linux Patches by CVE (no dupl)			
	Date Published		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	757	782	1
Average	270.376	31.367	8
Median	238	29	8
Average – Important	193.6	48.276	-
Median – Important	193	56	-
Average – Important (LifeLock)	193	36.429	-
Median – Important	193	30	-

(LifeLock)			

Linux Patches by CVE (no dupl)			
	Date Installed		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	1	1444	95
Average	26	151.657	107.305
Median	26	123.5	78
Average - Important	-	-	115.556
Median - Important	-	-	65
Average – Important (LifeLock)	-	-	128.529
Median – Important (LifeLock)	-	-	193

Linux Patches (no duplicates)			
	Date Published		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	549	591	1
Average	285.927	31.284	8
Median	282	29	8
Average – Important	193.6	45.417	-
Median – Important	193	53.5	-
Average – Important (LifeLock)	193	36.429	-
Median – Important (LifeLock)	193	30	-

Linux Patches (no duplicates)

	Date Installed		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	1	1083	57
Average	26	158.221	71.789
Median	26	34	56
Average – Important	-	-	70.966
Median – Important	-	-	56
Average – Important (LifeLock)	-	-	71.222
Median – Important (LifeLock)	-	-	31.5

There are 24 IP addresses that were identified as Microsoft by Gwenn and were on the PCI assessor's list. The following 16 IP addresses received at least one patch.

Name	IP Address
REDACTED	

REDACTED

The remaining 8 IPD addresses did not receive any patch. They are listed below:

Name	IP Address
REDACTED	

EXHIBIT H

Microsoft Patch Spreadsheet (PCI IP Addresses Only) – Summary Statistics				
	Importance of Patch (Microsoft Ratings)			
	All Data	Critical	Important	Moderate
Total Number	1929	839	1064	26
Percent of Whole	100	43.494	55.158	1.345
Mean	42.900	55.461	32.422	66.385
St. Dev	60.958	88.140	18.982	10.951
Lowest	1	1	1	31
25th percentile	15	15	17	66
Median	33	33	33	72
75th percentile	47	63	45	72
Highest	667	667	104	72
>30 days (#)	1234	465	743	26
>30 days (%)	63.971	55.423	69.831	100
>60 days (#)	290	229	39	22
>60 days (%)	15.034	27.294	3.665	84.615
>90 days (#)	133	107	26	0
>90 days (%)	6.895	12.753	2.444	0

Microsoft Patch Spreadsheet (PCI IP Addresses Only) – Summary Statistics					
	Importance of Patch (LifeLock Ratings)				
	All Data	Critical	Important	Med/Moderate	Low
Total Number	1929	763	1033	33	100
Percent of Whole	100	39.554	53.551	1.711	5.184
Mean	42.900	52.169	31.386	71.818	81.580
St. Dev	60.958	91.246	17.547	14.288	33.288
Lowest	1	1	1	31	58
25th percentile	15	10	17	68	58
Median	33	31	31	72	58
75th	47	62	45	72	92

percentile					
Highest	667	667	104	92	182
>30 days (#)	1234	387	714	33	100
>30 days (%)	63.971	50.721	69.119	100	100
>60 days (#)	290	194	23	29	44
>60 days (%)	15.034	25.426	2.227	87.879	44
>90 days (#)	133	72	10	7	44
>90 days (%)	6.895	9.436	0.968	21.212	44

Microsoft Patches (PCI IP Addresses Only)			
	Date Published		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	528	1149	252
Average	82.468	32.185	8.857
Median	62	33	8
Average - Critical	89.538	29.978	8.857
Median - Critical	61	34	8
Average – Critical (LL)	91.699	28.083	8.857
Median – Critical (LL)	62	34	8

Microsoft Patches (PCI IP Addresses Only)			
	Date Installed		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	375	592	962
Average	81.101	34.336	33.280

Median	58	17	33
Average - Critical	89.472	49.171	19.885
Median - Critical	58	35	15
Average – Critical (LL)	93.139	48.503	16.836
Median – Critical (LL)	58	35	15

Linux Patch Spreadsheet (PCI IP Addresses Only) – Summary Statistics				
	Importance of Patch (Linux Ratings)			
	All Data	**Important**	**Moderate**	**Low**
Total Number	39	17	13	9
Percent of Whole	100	43.590	33.333	23.077
Mean	82.231	79.294	89.231	77.667
St. Dev	70.413	65.633	95.709	2.87
Lowest	8	26	8	74
25th percentile	33	30	8	74
Median	67	56	48	78
75th percentile	81	67	81	81
Highest	283	196	283	81
>30 days (#)	30	13	9	9
>30 days (%)	76.923	76.471	69.231	100
>60 days (#)	19	5	6	9
>60 days (%)	48.718	29.412	46.154	100
>90 days (#)	7	4	3	0
>90 days (%)	17.949	23.529	23.077	0

Linux Patches (PCI IP Addresses Only)			
	Date Published		
	Before 12/1/12	From 12/1/12	On or after

		to 3/6/13	3/7/13
Number of Records	7	28	4
Average	220.289	58.321	8
Median	196	59	8
Average – Important	195.25	43.615	-
Median – Important	195	33	-

Linux Patches (PCI IP Addresses Only)			
	Date Installed		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	0	0	39
Average	-	-	81.575
Median	-	-	63
Average - Important	-	-	79.294
Median - Important	-	-	56

Linux Patches (no duplicates) (PCI IP Addresses Only) – Summary Statistics				
	Importance of Patch (Linux Ratings)			
	All Data	**Important**	**Moderate**	**Low**
Total Number	23	8	9	6
Percent of Whole	100	34.783	39.130	26.087
Mean	86.043	82.500	94.778	77.667
St. Dev	65.178	66.131	82.639	2.867
Lowest	8	26	8	74
25th percentile	45	30.75	43	74
Median	74	57.5	74	78
75th percentile	81	161.5	138	81
Highest	283	196	283	81
>30 days	20	6	8	6

(#)				
>30 days (%)	86.957	75	88.889	100
>60 days (#)	14	3	5	6
>60 days (%)	60.870	37.5	55.556	100
>90 days (#)	4	2	2	0
>90 days (%)	17.391	25	22.222	0

Linux Patches (no duplicates) (PCI IP Addresses Only) – Summary Statistics				
	Importance of Patch (LifeLock Ratings)			
	All Data	**Important**	**Moderate**	**Low**
Total Number	23	5	8	10
Percent of Whole	100	21.739	34.783	43.478
Mean	86.043	67.600	96.500	86.900
St. Dev	65.178	63.563	87.500	36.977
Lowest	8	26	8	59
25th percentile	45	28	42	72.25
Median	74	33	61	78
75th percentile	81	124.5	165.75	81
Highest	283	193	283	196
>30 days (#)	20	3	7	10
>30 days (%)	86.957	60	87.5	100
>60 days (#)	14	1	4	9
>60 days (%)	60.870	20	50	90
>90 days (#)	4	1	2	1
>90 days (%)	17.391	20	25	10

Linux Patches (no duplicates) (PCI IP Addresses Only)			
	Date Published		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	4	18	1
Average	216.75	61.333	8
Median	195.5	70.5	8
Average – Important	194.5	45.167	-
Median – Important	194.5	44.5	-
Average – Important (LL)	193	36.25	-
Median – Important (LL)	193	31.5	-

Linux Patches (no duplicates) (PCI IP Addresses Only)			
	Date Installed		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	0	0	23
Average	-	-	86.043
Median	-	-	74
Average - Important	-	-	82.5
Median - Important	-	-	57.5
Average – Important (LL)	-	-	67.6
Median – Important (LL)	-	-	33

Linux Patches by CVE (no dupl) (PCI IP Addresses Only) – Summary Statistics				
	Importance of Patch (Linux Ratings)			
	All Data	**Important**	**Moderate**	**Low**
Total	42	17	19	6

Number				
Percent of Whole	100	40.476	45.238	14.286
Mean	125.905	134.294	133.632	77.667
St. Dev	74.914	72.757	82.519	2.867
Lowest	8	26	8	74
25th percentile	67	57.5	74	74
Median	81	193	81	78
75th percentile	195	196	195	81
Highest	283	196	283	81
>30 days (#)	39	15	18	6
>30 days (%)	92.857	88.235	94.737	100
>60 days (#)	33	12	15	6
>60 days (%)	78.571	70.588	78.947	100
>90 days (#)	19	10	9	0
>90 days (%)	45.238	58.824	47.368	0

Linux Patches by CVE (no dupl) (PCI IP Addresses Only) – Summary Statistics				
	Importance of Patch (LifeLock Ratings)			
	All Data	**Important**	**Moderate**	**Low**
Total Number	42	9	17	16
Percent of Whole	100	21.429	40.476	38.095
Mean	125.905	123.333	139.824	112.563
St. Dev	74.914	78.277	85.125	56.556
Lowest	8	26	8	59
25th percentile	67	31.5	61	74
Median	81	193	195	81
75th percentile	195	193	195	196
Highest	283	193	283	196
>30 days (#)	39	7	16	16
>30 days	92.857	77.778	94.118	100

(%)				
>60 days (#)	33	5	13	15
>60 days (%)	78.571	55.556	76.471	93.75
>90 days (#)	19	5	9	5
>90 days (%)	45.238	55.556	52.941	31.25

Linux Patches by CVE (no dupl) (PCI IP Addresses Only)			
	Date Published		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	19	22	1
Average	204	63.818	8
Median	195	74	8
Average – Important	194.5	48.286	-
Median – Important	194.5	56	-
Average – Important (LL)	193	36.25	-
Median – Important (LL)	193	31.5	-

Linux Patches by CVE (no dupl) (PCI IP Addresses Only)			
	Date Installed		
	Before 12/1/12	From 12/1/12 to 3/6/13	On or after 3/7/13
Number of Records	0	0	42
Average	-	-	125.905
Median	-	-	81
Average - Important	-	-	134.294
Median -	-	-	193

Important			
Average – Important (LL)	-	-	123.333
Median – Important (LL)	-	-	193

EXHIBIT I

SEARCH Advanced Search ›

How do I know my information is secure with LifeLock?

LifeLock maintains a standards-based information security program that is designed to provide a high level of protection of member data. The security program includes the use of industry-standard encryption, active monitoring and response to potential attacks, pro-active assessments to discover and remediate potential system vulnerabilities and physical security mechanisms.

LifeLock maintains the highest level of PCI-DSS compliance

LifeLock is compliant as a Level 1 merchant under the PCI-DSS (Payment Card Industry Data Security Standard). PCI-DSS is a set of requirements that help protect cardholder data and is the accepted standard for all organizations that process credit card information.

Answer ID: 149 |

What is my Identity Exposure Level? How should I interpret my results?

Will a membership with LifeLock cover both my spouse and me?

Do you offer a family discount?

Does LifeLock or its employees use Peer-to-Peer (P2P) file sharing software?

Who is LifeLock?