



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Via email choofnagle@berkeley.edu

Chris Hoofnagle
UC Berkeley School of Law
344 Boalt Hall,
Berkeley, CA 94720

AUG 31 2016

Re: FOIA-2016-00255
Lifelock

Dear Mr. Hoofnagle:

This is in response to your request dated December 04, 2015, under the Freedom of Information Act seeking access to Lifelock's initial and biennial assessments and reports beginning in March 2010. In accordance with the FOIA and agency policy, we have searched our records as of December 18, 2015, the date we received your request in our FOIA office. This response will close this request and the 2012 and 2014 reports will be added to your pending FOIA request 2016-00804.

Your request did not indicate an agreement to pay any fees associated with the processing of your request. However, the Commission's fee regulations specify that fees less than \$25 will be waived. *See* 16 C.F.R. § 4.8(b)(4). Because the fees associated with the processing of your request did not exceed \$25, we have processed your request free of charge. In the future, please provide a fee agreement to facilitate the processing of your request.

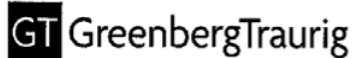
In addition, some responsive records constitute confidential commercial or financial information, which is exempt from disclosure under FOIA Exemption 4, 5 U.S.C. § 552(b)(4). Moreover, because Section 6(f) of the FTC Act, 15 U.S.C. § 46(f), prohibits public disclosure of this type of information, it is also exempt under FOIA Exemption 3, 5 U.S.C. § 552(b)(3), which, as noted above, exempts from disclosure any information that is protected from disclosure under another federal statute.

If you are not satisfied with this response to your request, you may appeal by writing to Freedom of Information Act Appeal, Office of the General Counsel, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580, within 90 days of the date of this letter. Please enclose a copy of your original request and a copy of this response. If you believe that we should choose to disclose additional materials beyond what the FOIA requires, please explain why this would be in the public interest. You also may seek dispute resolution services from the FTC FOIA Public Liaison Richard Gold, (202) 326-3355, rgold@ftc.gov or from the Office of Government Information Services via email ogis@nara.gov, via fax 202-741-5769, or via mail Office of Government Information Services (OGIS), National Archives and Records Administration, 8601 Adelphi Road, College Park, MD 20740-6001.

If you have any questions about the way we handled your request or about the FOIA regulations or procedures, please contact Anna Murray at (202) 326-2820.

Dione J. Stearns
Assistant General Counsel

Att: 1 pdf



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

November 18, 2010

Via Courier

Mr. James A. Kohm
Associate Director of Enforcement
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Room NJ-2122
Washington, DC 20580

Re: FTC v. LifeLock, Inc. and Richard Todd Davis;
Case: 2:10-cv-00530-NWW

Dear Mr. Kohm:

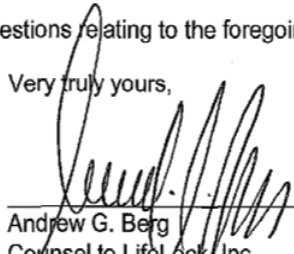
We represent LifeLock, Inc. ("LifeLock") and Richard Todd Davis in connection with the above-captioned matter.

LifeLock herein files this compliance report containing the mandated Information Security Program ("ISP") Assessment (Annex A) pursuant to Section III of the referenced Stipulated Final Judgment ("SFJ").

Due to the confidential nature of the ISP Assessment, LifeLock requests confidential treatment of this information; accordingly we have enclosed a public record version of this submission which deletes the contents of the referenced ISP Assessment.

Please advise if you have any questions relating to the foregoing.

Very truly yours,



Andrew G. Berg
Counsel to LifeLock, Inc.
and Richard Todd Davis

Enclosures

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

ALBANY
AMSTERDAM
ATLANTA
AUSTIN
BERLIN**
BOSTON
BRUSSELS**
CHICAGO
DALLAS
DELAWARE
DENVER
FORT LAUDERDALE
HOUSTON
LAS VEGAS
LONDON*
LOS ANGELES
MIAMI
MILAN**
NEW JERSEY
NEW YORK
ORANGE COUNTY
ORLANDO
PALM BEACH
COUNTY
PHILADELPHIA
PHOENIX
ROME**
SACRAMENTO
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
TALLAHASSEE
TAMPA
TYSONS CORNER
WASHINGTON, D.C.
WHITE PLAINS
ZURICH**

*OPERATES AS GREENBERG
TRAURIG MAHER LLP
**STRATEGIC ALLIANCE

Non-Public Version

Annex A



CHIEF SECURITY OFFICERS

www.ChiefSecurityOfficers.com

Non-Public Version

Date: November 17, 2010

To Whom It May Concern:

On March 15, 2010, the United States Federal Trade Commission (the "Commission") issued and filed a Stipulated Final Judgment and Order, Case No. 2:10-cv-00530-NVW (the "Order") against LifeLock, Inc. ("LifeLock").

In June 2010, Chief Security Officers, LLC (CSO) was engaged by LifeLock to conduct an independent review and assessment of LifeLock's ISP in accordance with the requirements under Section III of the FTC Order.

The review and assessment conducted by CSO covered the initial 180-day reporting period of March 15, 2010 through September 15, 2010. Physical on-site visits, interviews, testing and document and data sampling were conducted in two separate visits in August and September 2010.

The attached report is our assessment of LifeLock's ISP.

If you have any questions regarding the report please feel free to contact me at any time.

Respectfully,

Kenneth Rowe
Principal
Chief Security Officers
9821 N. 95th Street Suite 105
Scottsdale, Arizona 85258
888-237-3899
krowe@chiefsecurityofficers.com

Non-Public Version

CHIEF SECURITY OFFICERS, LLC INDEPENDENT ASSESSMENT OF LIFELOCK, INC.'S INFORMATION SECURITY PROGRAM

INITIAL REPORTING PERIOD
March 15, 2010 through September 15, 2010

On March 15, 2010, the United States Federal Trade Commission (the "Commission") issued and filed a Stipulated Final Judgment and Order, Case No. 2:10-cv-00530-NVW (the "Order") against LifeLock, Inc. ("LifeLock").

I. INTRODUCTION

The Information Security Program ("ISP") specified under Section II of the Order requires action on the part of LifeLock to ensure the following specific steps and processes are in place and operating as prescribed:

- a. Designation of an employee or employees to coordinate and be accountable for the ISP;
- b. Risk assessment to identify reasonably foreseeable internal and external threats to security, confidentiality and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information;
- c. Implementation of safeguards to control risks identified during the risk assessment; assessment of the safeguards in place to control certain risks and written reviews of the program, testing, monitoring effectiveness of the safeguards' key controls, systems, and procedures;
- d. Assurance that contractors or service providers are capable of maintaining appropriate safeguards for customer information by contractually requiring them to implement and maintain such safeguards;
- e. Adjustments to the program as key factors change.

Pursuant to Section III of the Order, LifeLock is required to obtain initial and biennial assessment reports ("assessments") from a qualified, objective, independent third party professional, who uses procedures and standards generally accepted in the profession.

Privileged and Confidential

Each assessment shall:

- a. Set forth the administrative, physical and technical safeguards implemented and maintained during the reporting period;
- b. Explain how safeguards implemented are appropriate;
- c. Explain how safeguards implemented meet or exceed the protections required in Section II of the Order; and
- d. Certify security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality and integrity of personal information is protected and has so operated throughout the reporting period.

II. INDEPENDENT REVIEW AND ASSESSMENT

In June 2010, Chief Security Officers, LLC (herein "CSO", "we", or "our") was engaged by LifeLock to conduct an independent review and assessment of LifeLock's ISP in accordance with the requirements under Section III of the Order.

The review and assessment conducted by CSO covered the initial 180-day reporting period of March 15, 2010 through September 15, 2010. Physical on-site visits, interviews, testing and document and data sampling were conducted in two separate visits in August and September 2010.

CSO Background, Experience and Qualifications

As required by the Order each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as Certified Information System Security Professional ("CISSP") or as a Certified Information Systems Auditor ("CISA"); a person holding Global Information Assurance Certification ("GIAC") from the SysAdmin, Audit, Security ("SANS") Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

As mandated by Section III of the Order, CSO meets or exceeds the requirements of the Order as all CSO security engineers have the required CISSP, CISA, PCI-QSA, and PA-QSA security certifications.

Privileged and Confidential

By way of background, CSO was formed in 2001 and is based in Scottsdale, Arizona. CSO provides a variety of security services to its customers including network vulnerability scanning, network penetration testing, PCI compliance assessments, ISO 27002 assessments, and HIPAA and Sarbanes Oxley compliance assessments. CSO is also a PCI Qualified Security Assessor ("QSA") company that is certified to provide onsite PCI assessments and PA-DSS Payment Application Testing, as well as a PCI Approved Scanning Vendor ("ASV"). As of September 26, 2010 CSO has performed security work for over 400 customers in 40 U.S. states, Mexico, Canada, and Argentina.

More information about CSO can be found at www.chiefsecurityofficers.com

III. PROCEDURES PERFORMED IN ASSESSING THE LIFELOCK ISP AND CONCLUSIONS

LifeLock's ISP is designed to protect the Security, Confidentiality, and Integrity of Personal Information. Administrative, Technical, and Physical Safeguards have been adopted to ensure the security of information of processed and stored on LifeLock's systems.

a. Set Forth The Administrative, Physical And Technical Safeguards Implemented And Maintained During The Reporting Period

Pursuant to Section III (a), this Section sets forth the administrative, physical and technical safeguards observed and confirmed to be implemented and maintained during the reporting period:

(i) Administrative Safeguards

ISO 27001

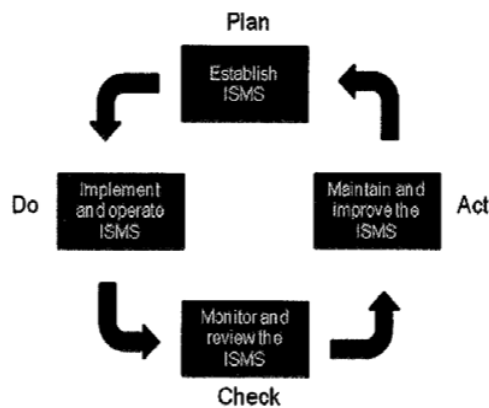
LifeLock maintains certification with the ISO 27001 standard of the International Standards Organization ("ISO") which provides much of the framework for the ISP and the company's compliance with the mandates of the Order. It is noteworthy that LifeLock's decision to seek and obtain this designation was voluntary and not required by applicable industry standards and regulations, and was implemented in advance of the implementation of the Order. LifeLock reports that the driving force behind the decision in 2007 (and continuing today) was the need to achieve and maintain the highest standard of security possible in its mission to become the leader in identity theft protection.

Privileged and Confidential

ISO 27001, formerly known as ISO/IEC 27001:2005 is the authoritative guidance and specification for the certification of an Information Security Management System ("ISMS"). The ISMS is a broad framework of policies and procedures that provide a systematic approach to manage security risks, and data protection over sensitive company and customer information so that it remains secure, confidential, accurate and available.

The initial certification was provided by LifeLock's independent certifying registrar and covered the three-year period from 2007 through 2009. In February 2010, LifeLock obtained recertification for another three-year period from 2010 through 2012.

LifeLock's ISMS under ISO 27001 is predicated on the Plan-Do-Check-Act ("PDCA") model, illustrated in the diagram below. We have confirmed that the ISMS is continually assessed for its operating effectiveness as well as any opportunities to improve its efficiency.



Plan (establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving Information security.
Do (implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and measure process performance against ISMS policy, and objectives and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audits and management review to achieve continual improvement of the ISMS.

Privileged and Confidential

LifeLock's use of this model has and currently provides the company the ability to generate a sustainable and repeatable means of measuring and managing risk as it provides guidance and direction over:

- Identification of critical information assets and asset owners;
- Specified vulnerabilities, threats and impacts to the information assets;
- Criteria for risk acceptance and residual risk; and
- Risk treatment plans.

PCI-DSS

Additionally, *we have confirmed* that LifeLock has maintained certification and compliance under the PCI DSS as a Level 1 merchant, which is the highest certification for a retail merchant processing greater than 6 million credit card transactions annually.

As required under this standard, LifeLock's certification is attested to by a QSA on an annual basis and is supported by a broad security program of technical and business processes including, but not limited to, vulnerability scanning, penetration tests, stringent access controls, formalized data classification and data protection policies, and service provider security management.

Designation of an employee or employees to coordinate and be accountable for the information security program

LifeLock's Information Security Steering Committee ("ISSC") is responsible for coordinating and being accountable for LifeLock's Information Security Program. The ISSC meets on at least a quarterly basis to manage and administer the program as documented by our review of meeting minutes during the compliance period.

Chaired by the Chief Information Officer ("CIO"), the ISSC also includes participation from the Associate General Counsel, the VP of Human Resources, and Director of Internal Audit. In addition to working collaboratively on the foundation of general ISSC initiatives, each member of the ISSC focuses on specific areas of the ISP that correspond to his or her area of expertise and corporate responsibilities.

The ISSC had memorialized one of its primary objectives and goals as being able to continually validate whether or not the program is operating as designed, with the intent to be sufficiently effective so that the security,

Privileged and Confidential

confidentiality, and integrity of personal information collected is properly protected given the factors of scalability and risk.

We verified the operation and function of the LifeLock Information Security Steering Committee ("ISSC") by reviewing the ISSC charter, documented meeting minutes, and interviewing members of the committee.

Risk Assessment

LifeLock identifies and assesses reasonably foreseeable, material internal and external risks to the security, confidentiality, and integrity of personal information and also assesses the sufficiency of safeguards in place to control identified risks. LifeLock conducts a range of assessments (ISO 27001, PCI), including some that focus specifically on information security and others that address broader subject matters of which information security is one component.

The ISP is designed to direct information security and privacy issues to the ISSC. On an ongoing basis, the ISSC assesses information security and privacy risks identified through the program. The Steering committee meets regularly, assigning resources and developing action plans to address identified risks, and following up on identified issues and action plans, as appropriate.

We verified LifeLock conducted a risk assessment using the NIST 800 framework by reviewing risks assessment reports and by interviewing LifeLock personnel. We also verified it is updated on at least an (b)(3) basis.

The risk assessment conducted for the ISP is the same of that conducted and required under its ISMS for ISO 27001 certification. This risk assessment methodology is based on the risk model under the NIST 800-30 – Risk Management Guide for Information Technology Systems, and is intended to identify and document reasonably foreseeable risks to personal information covered by the ISP. While other methodologies exist which are acceptable, given LifeLock's size and complexity, this methodology is widely used and accepted within the information technology industry and can be employed and tailored to companies of all sizes.

LifeLock also maintains a process for assessing risks and appropriate safeguards relating to the disclosure of personal information to service providers engaged in connection with new projects. This assessment process helps LifeLock determine the appropriate level of due diligence,

Privileged and Confidential

contractual obligations, and ongoing monitoring for service providers. *We verified that when a new service is offered, or a new vendor is considered, a risk assessment is conducted to confirm the ongoing security of LifeLock's systems.*

Other Administrative Safeguards:

Our review and assessment identified a number of additional administrative safeguards. These include:

Fraud Advisory Board

We verified that LifeLock has a Fraud Advisory Board comprised of industry security experts that advises them on the latest in security threats and trends by reviewing the list of members and confirming membership with one of its members.

Information Management Policies

We verified that LifeLock has developed extensive policies that were designed to protect the security, confidentiality, and integrity of personal information by reviewing this documentation and interviewing LifeLock personnel. Employees are required to sign an acceptable use policy and an employee handbook which outlines their responsibility for protecting personal information.

Information Classification

We verified that LifeLock as part of their risk assessment classifies its information and has policies and procedures in place for the appropriate handling of defined categories of information by reviewing these policies and procedures and interviewing LifeLock personnel.

Acceptable Use

We verified that LifeLock has developed an Acceptable Use Policy ("AUP") that defines the acceptable use of LifeLock's systems and identifies the consequences that will be imposed for a violation of the policy by reviewing the AUP and interviewing LifeLock personnel.

Workforce Security Responsibilities

We verified that LifeLock maintains controls for managing employees who have been provided varying levels of access to personal information by reviewing user access lists and by interviewing LifeLock personnel.

Privileged and Confidential

Security Awareness Training

We verified that LifeLock has developed a security awareness training program that is delivered at least annually and at initial hire by reviewing attendance lists and by reviewing contents of the actual program.

Service Provider Safeguards

In connection with executing and delivering its various service offerings to its members, LifeLock partners with multiple third party service providers. In some cases, it is necessary for these service providers either to receive, transmit, or store certain sensitive information of our members in helping LifeLock to fulfill a particular service.

We verified that LifeLock has a fully documented process to perform and obtain an appropriate level of due diligence to provide assurance that contractors or service providers are capable of maintaining appropriate safeguards before any new vendor is engaged by reviewing process documents and by interviewing LifeLock personnel.

This process included a formal Vendor Security Policy which outlines the procedures taken to adequately validate the risks and controls related to any new provider; which includes obtaining executed Non-Disclosure Agreements ("NDA's") and obtaining a Vendor Security Questionnaire to collect security information from the provider. Once all key risks and related controls have been reviewed and assessed, specific security measures or any special agreed-upon controls are documented as service level agreements within the respective contract(s). Any vendors who interact with any sensitive personal information of a member are required to sign a Privacy and Personal Information Protection Addendum, which requires specific privacy and data protection standards to be met by contractually requiring them to implement and maintain such safeguards.

Finally, in connection with our PCI-DSS Level 1 compliance, LifeLock conducts at least an annual review of its existing key service providers to ensure all vendors continue to demonstrate their security compliance and deliverables per their respective contractual agreements. This review consists primarily of obtaining and reviewing updated materials to corroborate security controls, including but not limited to, ISO 27001 certifications (as applicable), PCI-DSS compliance reports, vulnerability scans, other related audits or assessments and SAS 70 audit reports for hosted operations.

Privileged and Confidential

Incident Response

We verified that LifeLock has developed and implemented an incident response plan to ensure that all LifeLock employees know how to respond to an information security incident and that such response is compliant with existing laws and regulations by reviewing the plan and interviewing LifeLock personnel. The response plan is updated at least annually and tests are conducted to assess its effectiveness and is reviewed and assessed in light of any actual or suspected threats to the security, confidentiality, and integrity of personal information.

Business Continuity

We verified that LifeLock has a documented business continuity plan to address their critical business processes, along with the actions and resources required to provide continuity in service to its members in the case of an interruption by reviewing the plan and interviewing LifeLock personnel.

Termination Procedures

We verified that LifeLock has developed an asset management procedure to ensure that upon the termination of an employee, all company assets are returned and any access to personal information or other company information or data is immediately withdrawn by reviewing the procedure, interviewing LifeLock personnel, and reviewing termination paperwork for terminated employees.

Review of Access Rights

We verified that LifeLock performs reviews of access rights on at least a (b)(3): basis by reviewing access review reports and by interviewing LifeLock personnel.

(ii) Physical Safeguards

Hosted and Managed Data Center

We verified that LifeLock has all of its production systems housed in (b)(3):6(f),(b)(4) by conducting an onsite visit. The (b)(3): facility has tightly controlled (b)(3):6(f),(b)(4) (b)(3): (b)(4) has an annual (b)(3): audit performed that we have reviewed and deem to be adequate and compliant with industry standards.

Biometric Access

We verified that LifeLock has implemented biometric access in both of its facilities which require (b)(3):6(f),(b)(4) to

Privileged and Confidential

ensure that only authorized and authenticated individuals are granted access to its offices and contact center.

Visitor Access

We verified that LifeLock has a formalized process for controlling visitor access which requires all visitors to sign in at the reception desk and submit their driver's license before being given a temporary visitor badge. All visitors are required to be escorted at times while on the premises.

Asset Management

We verified that LifeLock maintains a database of hardware and software assets by reviewing asset reports and interviewing LifeLock personnel.

Removable Media

We verified that LifeLock protects removable media by reviewing (b)(3):6(f), (b)(4) reports and interviewing LifeLock personnel.

(iii) Technical Safeguards

Antivirus

We verified that LifeLock has installed (b)(3):6(f), (b) across the enterprise by reviewing antivirus reports and interviewing LifeLock personnel.

Change Control

We verified that LifeLock has a documented change control process in place by reviewing sample change control tickets and change control policy documentation.

Database Monitoring

We verified that LifeLock is monitoring access to its databases by reviewing Guardium reports and interviewing LifeLock personnel.

Encryption - Key Management

We verified that LifeLock encrypts sensitive information in its (b)(3) database by reviewing encrypted fields in the database and confirming the use of (b)(3):6(f). We also verified that LifeLock has a key management process in place by reviewing their Key Management Policy.

Privileged and Confidential

External Scanning

We verified that LifeLock is conducting external scanning at least quarterly by reviewing ISS external scan reports and confirming that the company is PCI compliant.

Internal Scanning

We verified that LifeLock is conducting internal scanning at least quarterly by reviewing ISS internal scan reports for the compliance period.

Scan for Personal Identifiable Information ("PII")

We verified that LifeLock regularly scans for unencrypted sensitive information on its network by reviewing (b)(3):6(f), (b)(4) reports during the compliance period.

Web Application Scanning

We verified that LifeLock is conducting web application scanning on a quarterly basis by reviewing Cenxic Hailstorm reports and the associated remediation to eliminate any high risk vulnerabilities.

Penetration Testing

We verified that LifeLock is conducting network layer penetration testing by reviewing (b)(3):6(f), (b)(4) reports during the compliance period.

Firewall

We verified that LifeLock has a documented firewall management program in place by reviewing firewall documentation and interviewing LifeLock personnel.

IDS/IPS

We verified that LifeLock has implemented IDS/IPS by reviewing IBM ISS reports for the compliance period and verifying that incidents are followed up on per its Incident Response Plan.

Incident Response (CIRT)

We verified that LifeLock has an incident response plan in place by reviewing their documented Incident Response plan and by interviewing LifeLock personnel. We confirmed that incidents noted during the compliance period were properly triaged and responded to as dictated by the Incident Response Plan.

Privileged and Confidential

Network Access Control

We verified that LifeLock has Network Access Control in place by reviewing NAC reports, interviewing LifeLock personnel and by attempting to connect a laptop to the LifeLock network.

Network segmentation

We verified that LifeLock has segmented its network and that sensitive information is stored in this segment by reviewing network diagrams and interviewing LifeLock personnel.

Password management

We verified that LifeLock has a secure password management program in place by reviewing documentation, interviewing LifeLock personnel, and reviewing print screens of password settings.

Patch Management

We verified that LifeLock has a patch management system in place by reviewing Microsoft WSUS and Altiris reports for the compliance period.

Two-Factor Authentication

We verified that LifeLock has two-factor authentication in place by reviewing VeriSign 2FA reports during the compliance period.

In addition to implementing and operating the safeguards described above, LifeLock also conducts other audits/reviews as described below.

Written Reviews of Tests, Monitoring and Effectiveness

As noted in the PDCA diagram in 3 (c) above, the ISMS is continually assessed for any corrective or preventive actions, as well as any efficiency improvement. Feedback for evaluation and adjustment comes from several internal and external sources, including but not limited to:

- Internal ISMS audits by LifeLock Internal Audit
- External audits from KPMG
- Semi-Annual ISO Surveillance Audits from accredited third party ISO Registrar Firm
- PCI Level 1 Audits from accredited third party QSA
- External legal compliance reviews from national law firm

In addition to conducting risk assessments, LifeLock regularly tests or otherwise reviews its information security systems and administrative functions to evaluate the effectiveness in controlling identified risks.

Privileged and Confidential

b. Explain How Safeguards Implemented Are Appropriate

Pursuant to Section III.A.2 of the Order, the safeguards implemented are appropriate for the following reasons:

LifeLock provided acceptable evidence and documentation for us to conclude that they have fully complied with all aspects of the Order for the initial reporting period. In many cases, LifeLock practices and security controls exceed industry best practices. We find that LifeLock has reasonably designed controls to meet the settlement terms on an ongoing basis. In our opinion LifeLock is materially and reasonably in compliance with the requirements cited in the Agreement.

It is our opinion the safeguards developed by LifeLock are appropriate for a company of its size and complexity. LifeLock has the same safeguards as other companies that are compliant with ISO 27001 and PCI-DSS Level 1.

LifeLock has also adopted the NIST framework for its risk assessment process which is an industry standard compliance framework.

c. Explain How Safeguards Implemented Meet Or Exceed The Protections Required In Section II Of The Order

Pursuant to Section III.A.3 of the Order, the safeguards implemented meet or exceed the protections required by Section II of the Order for the following reasons:

We have concluded that based on documentation and evidence provided by LifeLock and the procedures performed by CSO the implemented safeguards meet or exceed the protections required in Section II of the order.

Specifically it has:

- Pursuant to Section II, LifeLock has established a comprehensive information security program reasonably designed to protect the security, confidentiality, and integrity of personal information;
- Pursuant to Section II, LifeLock has documented the program in writing, including administrative, technical, and physical safeguards appropriate to LifeLock's size and complexity;
- Pursuant to Section II (a), LifeLock has designated an employee or employees to coordinate and be accountable for the program;
- Pursuant to Section II (b) LifeLock has identified material internal and external risks and the sufficiency of controls to mitigate those risks;
- Pursuant to Section II (c) LifeLock has designed and implemented reasonable safeguards and regularly test those controls;

Privileged and Confidential

- Pursuant to Section II (d) LifeLock has developed and used reasonable steps to retain service providers capable of safeguarding personal information entrusted to those service providers; and
 - Pursuant to Section II (e), LifeLock has adjusted the safeguards as needed based on testing and monitoring results.
- d. Certify Security Program Is Operating With Sufficient Effectiveness To Provide Reasonable Assurance That The Security, Confidentiality And Integrity Of Personal Information Is Protected And Has So Operated Throughout The Reporting Period

We believe that we have conducted adequate compliance testing as described herein, and based on our analysis and discussions with LifeLock, we are confident that LifeLock has adequately demonstrated the existence of a comprehensive information security program that is designed to protect the personal information of its customers and has so operated throughout the reporting period.

Pursuant to Section III.A.4, CSO hereby certifies that LifeLock's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

IV. DOCUMENTS AND RELATED MATERIALS REVIEWED BY CSO, LLC IN PERFORMING THE LIFELOCK ISP ASSESSMENT

Evidence Documents

- Altiris reports
- (b)(3):6(f) Print Screen
- (b)(3):6(f),(b)(1)
- Corrective and Preventive Action Procedure
- Current Network Diagram with Data Flows
- Data Exchange Agreements
- Employee New Hire Reports
- Employee Terminations
- Evidence of (b)(3): Removable Media Protection
- Evidence of User Access Review
- External Scan Reports
- Firewall logs from (b)(3):6
- Firewall Rules Review
- (b)(3):6(f),(b)(4)
- Guardium Logs

Privileged and Confidential

- Hardware Asset Matrix
- Incident Response Plan
- Internal Vulnerability Scan Reports
- ISSC Minutes
- ISSC Org/Charter
- List of Running Services
- Network Appliance Snapshot Reports
- (b)(3):6(f),(b)(4)
- (b)(3):6(f),(b)(4)
- Password Policy Print Screen for (b)(3):
- Password Policy Print Screen for (b)(3):6(f),(b)(4)
- PII Addendum
- PMO project Reports
- Sample Change Control Tickets
- Software Asset Matrix
- (b)(3):6(f),(b)(4)
- Tumbleweed (FTP) Logs
- VPN/VeriSign Logs
- White Hat Security Reports
- Windows Update Service ("WSUS") Reports

ISMS SCOPE

- ISMS Policy
- ISMS Scope
- Information Security Policy
- Statement of Applicability
- Management Review of ISMS Procedure
- Risk Assessment Procedure

SECURITY ORGANIZATION AND ISSC

- Information Security Organization Structure
- ISSC Charter and Mission Statement
- ISMS Security Awareness Training
- Privacy and Data Protection Awareness Training

ASSET AND DATA MANAGEMENT

- Information Assets-Owners Matrix
- Handling PII, PCI, and PHI Data Files
- Data Disposal Procedure
- Data Classification Labeling and Handling Procedure
- Encryption Key Management Procedure

Privileged and Confidential

- Document Control Procedure
- Preventing Data Leakage through Email Procedure

PHYSICAL SECURITY

- Mobile Computing Encryption Procedure
- Mobile Technology Policy
- Security Walkthrough Procedure

MONITORING, AUDIT & REVIEW

- Corrective and Preventive Action Plan Procedure
- Internal ISMS Audit Procedure
- Monitoring System Use Procedure

ACCESS

- Access Management Procedure
- Network Access Control Procedure
- Remote Access Procedure

NETWORK

- Firewall Change Control Procedure
- Infrastructure Cabling and Labeling Procedure
- LifeLock - Enterprise Diagram
- Network - PCI Environment Diagram
- Scheduled Database Backups Procedure
- Security Configuration Guide for Border Routers
- Security Configuration Guide for Firewalls
- Security Configuration Guide for Internal Routers and Switches
- System Backup Procedure
- Database Restore for Development, QA, & Prod Procedure
- Patch Management Procedure
- System Restart and Recovery Procedure

SERVICE PROVIDERS

- Vendor Security Policy
- LifeLock Vendor Security Questionnaire

CIRT/BCP

- General Computer Incident Response Procedure

Privileged and Confidential

SDLC/CHANGE MANAGEMENT

- Change Control Management Procedure
- Change Request Form
- Code Promotion to QA Procedure
- Capacity Management Procedure for Software Development Life Cycle ("SDLC")
- Process for Application Change Control
- System Deployment Procedure
- System Security Policy
- Release and Deployment Routing Instructions
- Subversion Commit Procedure

Privileged and Confidential

Page 17 of 17



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

November 18, 2010

Public Version

Via Courier

Mr. James A. Kohm
Associate Director of Enforcement
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Room NJ-2122
Washington, DC 20580

Re: FTC v. LifeLock, Inc. and Richard Todd Davis;
Case: 2:10-cv-00530-NWW

Dear Mr. Kohm:

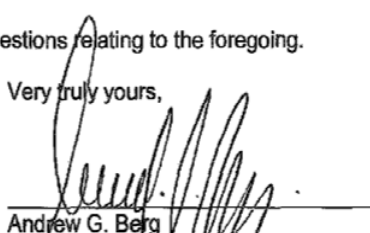
We represent LifeLock, Inc. ("LifeLock") and Richard Todd Davis in connection with the above-captioned matter.

LifeLock herein files this compliance report containing the mandated Information Security Program ("ISP") Assessment (Annex A) pursuant to Section III of the referenced Stipulated Final Judgment ("SFJ").

Due to the confidential nature of the ISP Assessment, LifeLock requests confidential treatment of this information; accordingly we have enclosed a public record version of this submission which deletes the contents of the referenced ISP Assessment.

Please advise if you have any questions relating to the foregoing.

Very truly yours,


Andrew G. Berg
Counsel to LifeLock, Inc.
and Richard Todd Davis

Enclosures

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

ALBANY
AMSTERDAM
ATLANTA
AUSTIN
BERLIN**
BOSTON
BRUSSELS**
CHICAGO
DALLAS
DELAWARE
DENVER
FORT LAUDERDALE
HOUSTON
LAS VEGAS
LONDON*
LOS ANGELES
MIAMI
MILAN**
NEW JERSEY
NEW YORK
ORANGE COUNTY
ORLANDO
PALM BEACH
COUNTY
PHILADELPHIA
PHOENIX
ROME**
SACRAMENTO
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
TALLAHASSEE
TAMPA
TYSONS CORNER
WASHINGTON, D.C.
WHITE PLAINS
ZURICH**
*OPERATES AS GREENBERG
TRAURIG MAHER LLP
**STRATEGIC ALLIANCE

Public Version

Annex A



www.ChiefSecurityOfficers.com

Public Version

Date: November 17, 2010

To Whom It May Concern:

On March 15, 2010, the United States Federal Trade Commission (the "Commission") issued and filed a Stipulated Final Judgment and Order, Case No. 2:10-cv-00530-NVW (the "Order") against LifeLock, Inc. ("LifeLock").

In June 2010, Chief Security Officers, LLC (CSO) was engaged by LifeLock to conduct an independent review and assessment of LifeLock's ISP in accordance with the requirements under Section III of the FTC Order.

The review and assessment conducted by CSO covered the initial 180-day reporting period of March 15, 2010 through September 15, 2010. Physical on-site visits, interviews, testing and document and data sampling were conducted in two separate visits in August and September 2010.

The attached report is our assessment of LifeLock's ISP.

If you have any questions regarding the report please feel free to contact me at any time.

Respectfully,

Kenneth Rowe
Principal
Chief Security Officers
9821 N. 95th Street Suite 105
Scottsdale, Arizona 85258
888-237-3899
krowe@chiefsecurityofficers.com

Public Version

CHIEF SECURITY OFFICERS, LLC INDEPENDENT ASSESSMENT OF LIFELOCK, INC.'S INFORMATION SECURITY PROGRAM

INITIAL REPORTING PERIOD
March 15, 2010 through September 15, 2010

On March 15, 2010, the United States Federal Trade Commission (the "Commission") issued and filed a Stipulated Final Judgment and Order, Case No. 2:10-cv-00530-NVW (the "Order") against LifeLock, Inc. ("LifeLock").

Due to the confidential nature of the information, the contents of the ISP Assessment report is redacted.