**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 __8__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

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?

**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 __9__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

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

MileagePlus
UNITED

PRSRT STD
U.S Postage
PAID
LIFELOCK

Exclusive Offer Enclosed for
United MileagePlus® Member:

<First Name><Last Name>
<Address Line 1>
<Address Line 2>
<Address Line 3>
[[[[[[[[ BAR CODE ]]]]]]]]]

**How many times today will you open up your personal life to the risk of identity theft?**

*The information inside will surprise you...*

#11 OME_10.375w x 4.5h
window die: 4.5w x 1.25h
L = 0.875, B = 0.5

MileagePlus
UNITED

# Everyone should know their personal risk for identity theft–even you, <Sample A. Sample>.

Because there's a new victim every 3 seconds.[1]

<First Name><Last Name>
<Address Line 1>
<Address Line 2>
<Address Line 3>
[[[[[[[[ BAR CODE ]]]]]]]]]

Dear <Sample A. Sample>,

Every time you pay with your credit card, deposit or withdraw money at an ATM, log onto the Internet, use a smartphone or post a message through social media ... you open yourself up to identity theft.

From your financial transactions to your passwords, confidential information about you is transmitted electronically across town, across the country or even to some other part of the world.

*Once it's out of your hands, this sensitive data is at risk for unauthorized access or potential exploitation by cyber-thieves. But do you really need to be concerned?* After all, don't credit card companies, financial institutions and businesses have rigid security procedures in place?

**Tell that to the 11.6 million Americans who in 2011 experienced the crime of identity theft—over 1.4 million more victims than the previous year.**[1]

These honest, unassuming victims thought their account numbers, passwords and other personal data were safe from identity thieves. Instead, they were violated by a variety of security crimes. For some, it took days, weeks or months to clear their good name and restore their life. Identity fraud in the U.S. added up to a cost of $18 billion in 2011.[1]

**That's why you should defend yourself with LifeLock® Identity Theft Protection. United MileagePlus® members receive 10% OFF* and up to 5,000 bonus miles.****

LifeLock is America's leader in identity theft protection—the first truly proactive defense system for individuals and their families. Your LifeLock membership will provide these vital benefits:

1. **LifeLock Identity Alerts:** An "early warning system" that alerts you of potential misuse of your personal information.†
2. **Advanced Internet Monitoring:** Proactively monitors over 10,000 black market websites where stolen personal account and identification numbers are bought and sold.

*over, please*

LifeLock
Relentlessly Protecting Your Identity™

## LifeLock Identity Theft Protection helps stop the misuse of your personal information before it happens.

**As a United MileagePlus® member, you are entitled to this exclusive offer:**

- **10% OFF*=$9/month LifeLock Identity Theft Protection**
- **Earn up to 5,000 MileagePlus bonus miles****

**Call 1-800-613-5774 now or visit LifeLock.com**

**Use promo code: UNITED12**
**Act by January 1, 2013**

*Offer is for new LifeLock members only. Pricing refers to standard LifeLock identity theft protection only and does not include applicable sales tax.

3. **Lost Wallet Protection:** Replaces not only credit cards but also driver's licenses and other official documents if your wallet is ever lost or stolen. (Excludes pictures, cash and cash equivalents.)

4. **Personalized Online Dashboard:** Provides you with anytime access to your alerts via the secure LifeLock Member Portal.

5. **$1,000,000 Total Service Guarantee:** If you become a victim of identity theft, LifeLock will spend up to $1 million to hire experts, lawyers, investigators, consultants and whomever else it takes to help your recovery.‡

As a member of United MileagePlus, take advantage of this exclusive offer to save 10%* on LifeLock membership and earn up to 5,000 bonus miles** Call **1-800-613-5774** or visit **LifeLock.com**. Use promo code **UNITED12** to receive your special privileges.

Sincerely,

David Oppenheim
Managing Director, MileagePlus

P.S. Remember, your favorite destination is now as much as 5,000 MileagePlus miles closer when you protect your personal information with LifeLock. Hurry—this exclusive offer ends on January 1, 2013.

## Enroll now. It's quick. It's easy. It's secure.

### 10% OFF* LifeLock membership AND earn up to 5,000 MileagePlus bonus miles**

Enrollment takes just minutes online or by phone.
**1-800-613-5574** or visit **LifeLock.com** Use promo code: **UNITED12**

*Offer is for new LifeLock members only. Pricing refers to standard LifeLock identity theft protection only and does not include applicable sales tax.

**Must be an active LifeLock member for 31 days to earn miles. Please allow 6-8 weeks for mile to post to your account. United members will earn 2,500 United miles for the first year of standard LifeLock identity theft protection enrollment and 1,250 miles for membership years 2 and 3. United members will earn 3,000 United m les for the first year of LifeLock Ultimate™ enrollment and 1,250 miles for membership years 2 and 3. Additional bonus award miles for years two and three w ll be posted to the member's account at the beginning of each of the respective membership years. Members may cancel at any time without penalty by calling 1-800-LifeLock.

Miles accrued and awards issued are subject to the rules of the United MileagePlus program. United and its subsidiaries, affiliates and agents are not responsible for any products and services of other participating companies and partners. The M leagePlus program, including accruals, awards and bonus miles offers is subject to change without notice. Taxes and fees related to award travel are the responsibility of the passenger. United and MileagePlus are registered service marks. For complete details about the MileagePlus program, go to www.united.com

† Network does not cover all transactions and scope may vary.

‡ The benefits under the Service Guarantee are provided under a Master Insurance Policy underwritten by State National Insurance Company. As this is only a summary please see the actual insurance policy for applicable terms and restrictions at LifeLock.com.

§ "2012 Identity Fraud Survey Report"; Javelin Strategy & Research, February 2012

**Gene Z.**
**LifeLock member**

"LifeLock's protection has made me feel very safe about my identity ... two incidents later and no damage ... and taking care of it without me having to jump through hoops. I really appreciated that."

**Michele C.**
**LifeLock member**

"Somebody got a copy of my driver's license and they went ahead and manufactured a bunch of false checks. They took them to a brand name store and cashed checks that were approved. A very good friend of mine said I should sign up for LifeLock..."

**Justin L.**
**LifeLock member**

"I got a call from a credit card company saying, 'We want to verify this application that you applied for.' I said, 'I don't know who you are. I never applied for anything.' That started about a six month nightmare. I said enough is enough and signed up for LifeLock... "

LifeLock®
Relentlessly Protecting Your Identity™

LifeLock
Relentlessly Protecting Your Identity.

See inside
to learn how

# IF IT'S PERSONAL TO YOU, KEEP IT PRIVATE.

## Guard your sensitive information with LifeLock® Identity Theft Protection.

MileagePlus
UNITED

## How LifeLock works to keep your identity more secure

- **Monitors proactively** to uncover if your name or personal information is being used to open new accounts without your knowledge.†
- **Scans criminal Internet sites** for the illegal buying, selling or trading of your personal information.
- **Alerts you** if we detect that your personal information may have been used and assigns a risk level.†
- **Helps stop fraudulent charges** and cancel or replace your credit cards if your wallet is lost or stolen.
- **Provides direct access** to special identity theft Member Services Agents to work with you until you're satisfied that your good name is secure.

*Offer is for new LifeLock members only. Pricing refers to standard LifeLock identity theft protection only and does not include applicable sales tax.
**Must be an active LifeLock member for 31 days to earn miles. Please allow 6-8 weeks for miles to post to your account. United members will earn 2,500 United miles for the first year of standard LifeLock identity theft protection enrollment and 1,250 miles for membership years 2 and 3. United members will earn 3,000 United miles for the first year of LifeLock Ultimate™ enrollment and 1,250 miles for membership years 2 and 3. Additional bonus award miles for years two and three will be posted to the member's account at the beginning of each of the respective membership years. Members may cancel at any time without penalty by calling 1-800-LifeLock. Miles accrued and awards issued are subject to the rules of the United MileagePlus program. United and its subsidiaries, affiliates and agents are not responsible for any products and services of other participating companies and partners. The MileagePlus program, including accruals, awards and bonus miles offers is subject to change without notice. Taxes and fees related to award travel are the responsibility of the passenger. United and MileagePlus are registered service marks. For complete details about the MileagePlus program, go to www.united.com
† Network does not cover all transactions and scope may vary.

MileagePlus
UNITED

LifeLock
Relentlessly Protecting Your Identity™

## *Wherever you go, whatever you do...*
## The risks of becoming a victim of identity theft are everywhere.

When you use your credit card

When you use wireless Internet at home or away

When you use an ATM machine

When you dispose of mail without shredding it

When you have personal data stored on your Smartphone

When you throw out, recycle or donate an old computer

When you post personal information on social media sites

**And thieves seeking to violate your financial security have no shortage of tactics–from simple to sophisticated.**

They steal credit and debit card numbers using a device attached to ATM machines that reads the magnetic strip. They divert your billing statements to another location by completing a change of address form. They go through your trash looking for bills, credit cards and other information. They get personal information from old computer hard drives. ***Bottom line: Their methods are endless and ever-changing.***

While there's no way to escape the risks of identity theft, you can protect yourself with LifeLock® Identity Theft Protection–the first truly proactive defense system for individuals and their families. ***Get started now!***

MileagePlus
UNITED

**Call 1-800-613-5574 or visit LifeLock.com**

Use promo code **UNITED12** to receive this exclusive offer:

✓ 10% OFF*=$9/month

✓ Earn up to 5,000 MileagePlus® bonus miles**

LifeLock
Relentlessly Protecting Your Identity™

LifeLock®
Relentlessly Protecting Your Identity™

**Special offer enclosed for Hilton HHonors™ members.**
**ACTION REQUESTED BY JANUARY 1, 2013.**

‹John Q. Sample›
‹Address line 1›
‹Address line 2›
‹Address line 3›
‹Bar Code›

**Special Offer for**
**Hilton HHonors Members:**
**30 Days FREE***
**+ 10% OFF = $9/MONTH**
**LIFELOCK IDENTITY THEFT PROTECTION**
**AND**
**Earn up to 5,800 Hilton HHonors Bonus Points!****

Dear ‹First› ‹Last›,

Three seconds. The time it takes for another American to fall victim to identity theft, classified by the Social Security Administration as *"one of the fastest growing crimes in America."*[1] Ten years ago you didn't hear much about identity theft. Nowadays, common tasks like sending an email, shopping online or using a credit card can leave you, your credit and your finances vulnerable to attack.

That is why I am pleased to introduce you to an exciting benefit for Hilton HHonors members that works 24/7/365 to defend you from identity theft before it happens: **LifeLock® identity theft protection.**

While no one can prevent all identity theft, LifeLock protects against many of the most serious types of identity theft.† Their sophisticated technology works tirelessly to help protect you both online and offline by:

- Alerting you when LifeLock detects your information in applications for utility, cell phone and credit accounts within the extensive LifeLock network.†
- Patrolling criminal Internet sites for the illegal buying, selling or trading of your personal information.
- Assisting you in canceling and replacing lost or stolen credit cards to help stop fraudulent charges.

And if LifeLock doesn't protect you from identity theft, we will spend up to $1,000,000 to hire experts, lawyers and whomever else necessary to help your recovery.‡

Best of all, with LifeLock service, the next time you make a purchase, bank online or go to a restaurant, you can do so with confidence—at home or while traveling.

**Act now and get A SPECIAL OFFER of just $9 a month, a savings of 10%, when you sign up for LifeLock identity theft protection membership before January 1, 2013.** Use promo code **HHONORS1** and you will get your first 30 days of LifeLock membership **FREE*** plus earn up to 5,800 Hilton HHonors Bonus Points.** After the first 30 days, you'll be billed automatically at the discounted price of just $9 a month or $99 a year plus applicable sales tax for standard membership—unless you cancel within the first 30 days by calling 1-800-LifeLock.

Identity theft is real and so are the consequences. I urge you to protect yourself with LifeLock service today.

Sincerely,

Todd Davis

Todd Davis, CEO, LifeLock

P.S. **In the time it takes you to read this sentence, another identity may be stolen.** Do not wait. It only takes minutes to sign up, but act before January 1, 2013 to take part in this special offer. Call 1-800-647-7134 or visit LifeLock.com now.

*At the end of the first 30 days, your card will be billed automatically ($9mo/$99yr plus applicable sales tax for standard LifeLock membership) unless you cancel within the 30-day trial period. You can cancel anytime without penalty by calling 1-800-LifeLock. Offer is for new LifeLock members only.

**Protect your identity with LifeLock service today:**

**Proactive identity threat alerts**

**Advanced Internet threat detection**

**Lost or stolen wallet protection**

**24/7/365 access to a live Member Services Agent**

**And more!**

**Enroll Now:**
**1-800-647-7134**
**LifeLock.com**

†Network does not cover all transactions and scope may vary.

‡The benefits under the Service Guarantee are provided under a Master Insurance Policy underwritten by State National Insurance Company. As this is only a summary please see the actual policy for applicable terms and restrictions at LifeLock.com.

**You must sign up for LifeLock services using the steps described herein and promo code "HHonors1" to receive this offer. Must be an active LifeLock member for 31 days to earn Hilton HHonors Bonus Points. No Hilton HHonors Bonus Points will be awarded for memberships canceled during the 30-day trial period. Please allow six-eight weeks for Hilton HHonors Bonus Points to be credited to your account. Hilton HHonors members will earn 3,500 HHonors Bonus Points for the first year of standard LifeLock identity theft protection upon completion of the trial period. Members will earn 1,150 HHonors Bonus Points for standard membership years two and three upon payment for each respective year. Hilton HHonors members will earn 5,000 HHonors Bonus Points for the first year of LifeLock Ultimate enrollment upon completion of the trial period. Members will earn 1,150 HHonors Bonus Points for LifeLock Ultimate membership years two and three upon payment for each respective year. Hilton HHonors Bonus Points do not count toward elite tier qualification. Hilton HHonors™ membership, earning of Points & Miles™ and redemption of Points are subject to HHonors Terms and Conditions, HHonors.com/Terms.

[1] Statistics based on identity fraud figures in the "2012 Identity Fraud Survey Report"; Javelin Strategy & Research, February 2012 and "Identity Theft And Your Social Security Number"; Social Security Administration, August 2009.

## SPECIAL OFFER FOR HILTON HHONORS MEMBERS

HILTON HHONORS

☑ 10% OFF the Regular Price

☑ BONUS! 30 Days of LifeLock Membership

☑ Earn up to 5,800 Hilton HHonors Bonus Points**

**Enroll Before January 1, 2013!**

**Name:**
‹First› ‹Last›

**Enroll now—quickly, easily and securely:**
**LifeLock.com** or **1-800-647-7134**

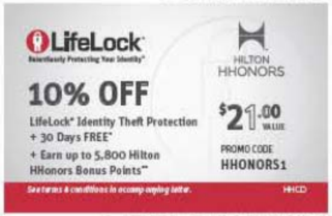
**Use promotion code:**
**HHONORS1**

DM10 HH-DM1

LCTRL-0812

LifeLock®
Relentlessly Protecting Your Identity™

CONFIDENTIAL



LifeLock

Relentlessly Protecting Your Identity®

# 10% OFF

LifeLock® Identity Theft Protection
+ 30 Days FREE*
+ Earn up to 5,800 Hilton HHonors Bonus Points℠

HILTON HHONORS

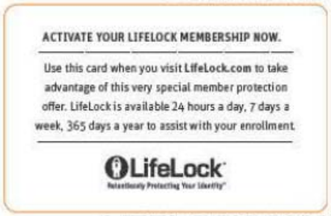
$21.00 VALUE

PROMO CODE
HHONORS1

See terms & conditions in accompanying letter.

HHCD

CONFIDENTIAL

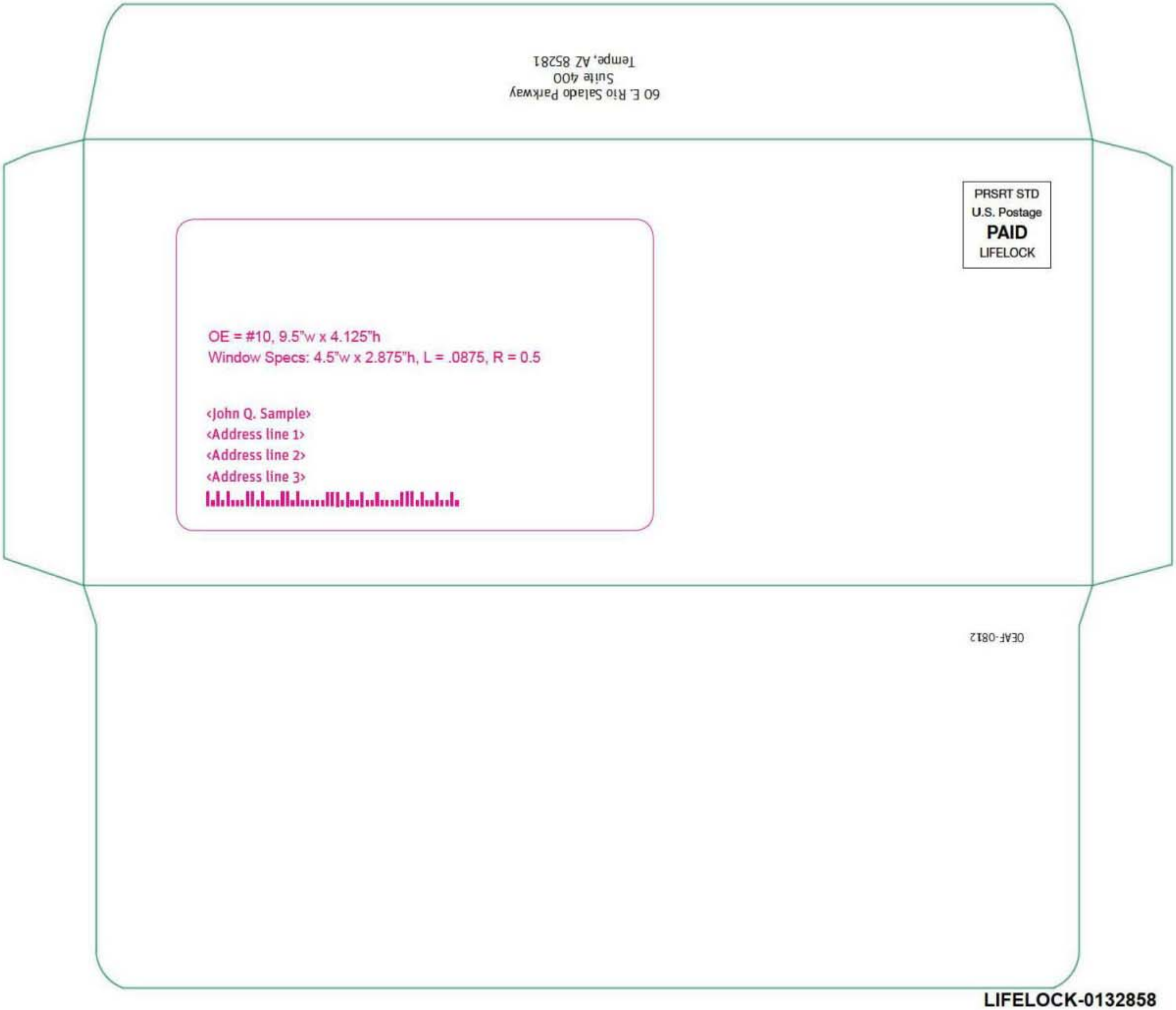


ACTIVATE YOUR LIFELOCK MEMBERSHIP NOW.

Use this card when you visit LifeLock.com to take advantage of this very special member protection offer. LifeLock is available 24 hours a day, 7 days a week, 365 days a year to assist with your enrollment.

LifeLock

Relentlessly Protecting Your Identity



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

PRSRT STD
U.S. Postage
**PAID**
LIFELOCK

OE = #10, 9.5"w x 4.125"h
Window Specs: 4.5"w x 2.875"h, L = .0875, R = 0.5

‹John Q. Sample›
‹Address line 1›
‹Address line 2›
‹Address line 3›

OEAF-0812

Protect What Matters Most
With LifeLock® Identity Theft Protection

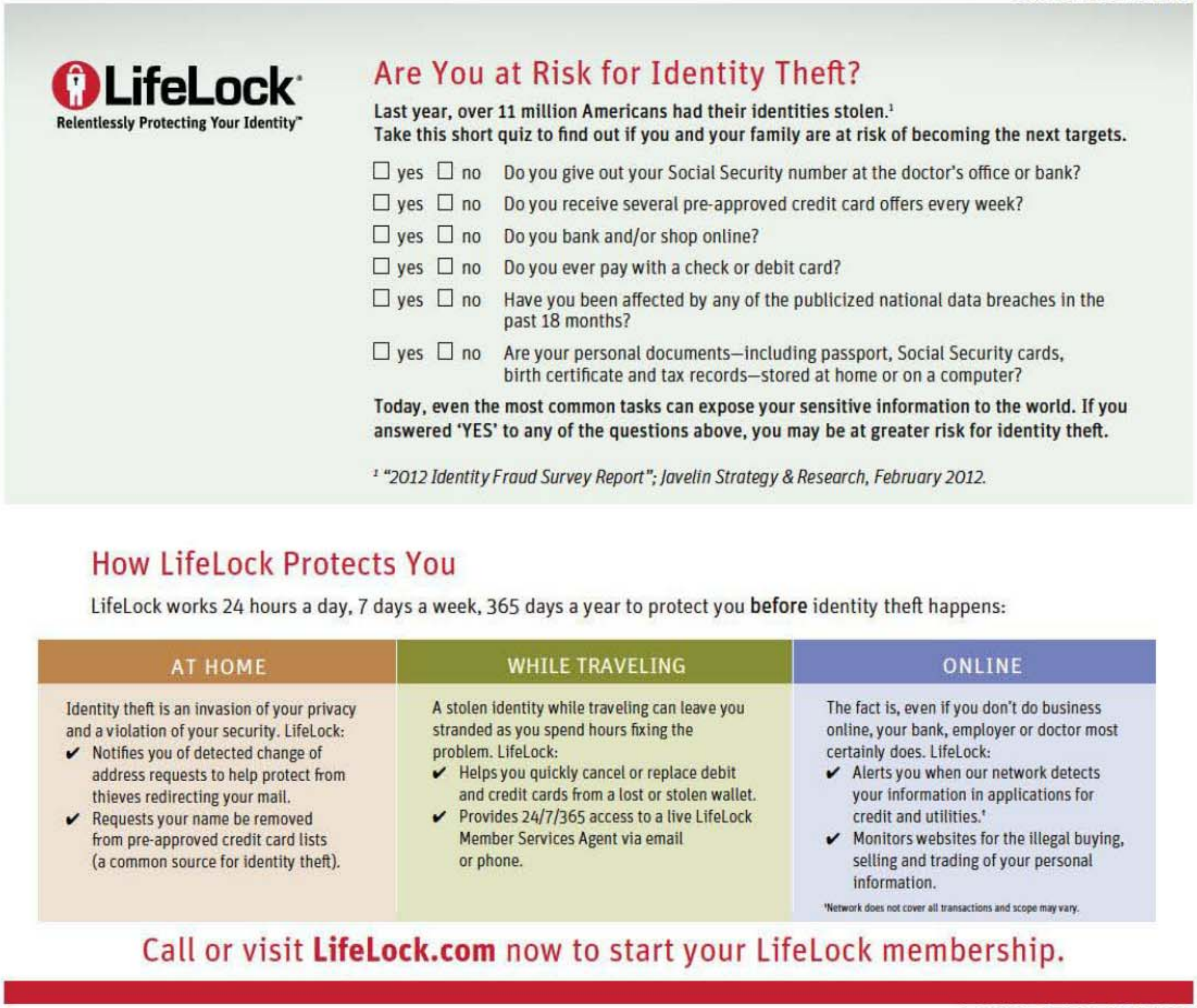
LifeLock®
Relentlessly Protecting Your Identity™

## Protect Your Identity Today.
## Start Your LifeLock® Membership Now.

Enrollment is quick and easy. Just use the enclosed enrollment card to take advantage of your special offer.

LifeLock®
Relentlessly Protecting Your Identity™

BROAF-0812



LifeLock

Relentlessly Protecting Your Identity™

## Are You at Risk for Identity Theft?

**Last year, over 11 million Americans had their identities stolen.[1]**
**Take this short quiz to find out if you and your family are at risk of becoming the next targets.**

□ yes □ no Do you give out your Social Security number at the doctor's office or bank?

□ yes □ no Do you receive several pre-approved credit card offers every week?

□ yes □ no Do you bank and/or shop online?

□ yes □ no Do you ever pay with a check or debit card?

□ yes □ no Have you been affected by any of the publicized national data breaches in the past 18 months?

□ yes □ no Are your personal documents–including passport, Social Security cards, birth certificate and tax records–stored at home or on a computer?

**Today, even the most common tasks can expose your sensitive information to the world. If you answered 'YES' to any of the questions above, you may be at greater risk for identity theft.**

[1] *"2012 Identity Fraud Survey Report"; Javelin Strategy & Research, February 2012.*

## How LifeLock Protects You

LifeLock works 24 hours a day, 7 days a week, 365 days a year to protect you **before** identity theft happens:

### AT HOME

Identity theft is an invasion of your privacy and a violation of your security. LifeLock:

- ✔ Notifies you of detected change of address requests to help protect from thieves redirecting your mail.
- ✔ Requests your name be removed from pre-approved credit card lists (a common source for identity theft).

### WHILE TRAVELING

A stolen identity while traveling can leave you stranded as you spend hours fixing the problem. LifeLock:

- ✔ Helps you quickly cancel or replace debit and credit cards from a lost or stolen wallet.
- ✔ Provides 24/7/365 access to a live LifeLock Member Services Agent via email or phone.

### ONLINE

The fact is, even if you don't do business online, your bank, employer or doctor most certainly does. LifeLock:

- ✔ Alerts you when our network detects your information in applications for credit and utilities.*
- ✔ Monitors websites for the illegal buying, selling and trading of your personal information.

*Network does not cover all transactions and scope may vary.

Call or visit **LifeLock.com** now to start your LifeLock membership.

**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 __10_ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

LifeLock® U·S AIRWAYS® DIVIDEND MILES

**Benefit information enclosed for US Airways® Dividend Miles members. ACTION REQUESTED BY MAY 1ST, 2013.**

‹John Q. Sample›
‹Address line 1›
‹Address line 2›
‹Address line 3›
‹Bar Code›

**Special Offer for**
**US Airways® Dividend Miles members:**
**30 Days FREE***
**+ 10% OFF = $9/MONTH**
LIFELOCK IDENTITY THEFT PROTECTION
**AND**
Earn up to 3,000
US Airways Dividend miles!**

Dear ‹First› ‹Last›,

Three seconds. That's the time it takes for another unsuspecting American to become a casualty of identity theft, a crime that victimized nearly one in twenty U.S. adults in 2011.[1] Ten years ago you didn't hear much about identity theft. Nowadays, common tasks like sending an email, shopping online or using a credit card can leave you, your credit and your finances vulnerable to attack.

That is why we are pleased to introduce you to an exciting benefit for US Airways Dividend Miles members that works 24/7/365 to defend you from identity theft before it happens: **LifeLock® identity theft protection.**

While no one can prevent all identity theft, LifeLock protects against many of the most serious types of identity theft.† The sophisticated technology works tirelessly to help protect you both online and offline by:

- Alerting you when LifeLock detects your information in applications for utility, cell phone and credit accounts within the extensive LifeLock network.†
- Patrolling criminal Internet sites for the illegal buying, selling or trading of your personal information.
- Assisting you in canceling and replacing lost or stolen credit cards to help stop fraudulent charges.

And if LifeLock doesn't protect you from identity theft, Lifelock will spend up to $1,000,000 to hire experts to help your recovery.‡

Best of all, with LifeLock service, the next time you make a purchase, bank online or go to a restaurant, you can do so with confidence—at home or while traveling.

**Act now and get A SPECIAL OFFER of just $9 a month, a savings of 10%, when you sign up for LifeLock identity theft protection membership before May 1, 2013.** Use promo code **TRAVEL75** and you will also get your first 30 days of LifeLock membership **FREE*** and earn up to 3,000 miles.** After the first 30 days, you'll be billed automatically at the discounted price of just $9 a month or $99 a year plus applicable sales tax for standard membership—unless you cancel within the first 30 days by calling 1-800-LifeLock.

Identity theft is real and so are the consequences. We urge you to protect yourself with LifeLock service today.

Sincerely,

Todd Davis
CEO, Lifelock

Fernand Fernandez
US Airways Managing Director,
Marketing and Customer Loyalty

P.S. **In the time it takes you to read this sentence, another identity may be stolen.** Do not wait. It only takes minutes to sign up, but act before May 1, 2013 to take part in this special offer. Call 1-800-430-1014 or visit LifeLock.com now.

*At the end of the first 30 days, your card will be billed automatically ($9mo/$99yr plus applicable sales tax for standard LifeLock membership) unless you cancel within the 30-day trial period. You can cancel anytime without penalty by calling 1-800-LifeLock. Offer is for new LifeLock members only.

**Protect your identity with LifeLock service today:**

**Proactive identity threat alerts**

**Advanced Internet threat detection**

**Lost or stolen wallet protection**

**24/7/365 access to a live Member Services Agent**

**And more!**

**Enroll Now:**
**1-800-430-1014**
**LifeLock.com**

†Network does not cover all transactions and scope may vary.

‡The benefits under the Service Guarantee are provided under a Master Insurance Policy underwritten by State National Insurance Company. As this is only a summary please see the actual policy for applicable terms and restrictions at LifeLock.com.

**US Airways Dividend Miles: Must be an active LifeLock member to earn Dividend Miles. This offer is exclusive to new adult LifeLock members who have not been members within the last 12 months. After the 30 day trial, you will be awarded 3,500 bonus miles with annual adult/1,000 bonus miles with monthly adult LifeLock Ultimate™ membership or 3,000 bonus miles with annual adult/750 bonus miles with monthly adult LifeLock® identity theft protection membership. Please allow 6-8 weeks for miles to be credited to your account. US Airways is not responsible for the quality or delivery of goods and/or services provided by LifeLock or any other Dividend Miles partner. All Dividend Miles Terms and Conditions apply.

[1] "2012 Identity Fraud Survey Report"; Javelin Strategy & Research, February 2012.

## SPECIAL OFFER FOR US AIRWAYS DIVIDEND MILES MEMBERS

U·S AIRWAYS® DIVIDEND MILES

☑ 10% OFF the Regular Price

☑ 30 Days FREE* of LifeLock Membership

☑ PLUS, up to 3,000 US Airways Dividend Miles!**

**Enroll Before May 1, 2013!**

**Name:**
‹First› ‹Last›

**Enroll now—quickly, easily and securely:**
**LifeLock.com** or **1-800-430-1014**

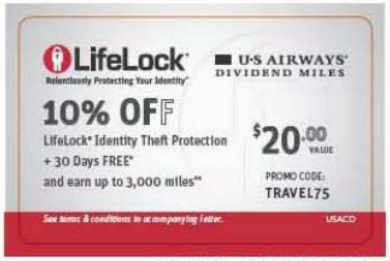
**Use promotion code:**
**TRAVEL75**

DM02 USA-DM1

LCTRL-0113

LifeLock®
Relentlessly Protecting Your Identity®

CONFIDENTIAL



LifeLock®

Relentlessly Protecting Your Identity®

U·S AIRWAYS®
DIVIDEND MILES

10% OFF

LifeLock® Identity Theft Protection
+ 30 Days FREE*
and earn up to 3,000 miles**

$20.00 VALUE

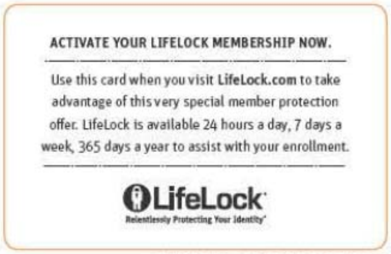
PROMO CODE:
TRAVEL75

*See terms & conditions in accompanying letter.*

USACD

LIFELOCK-0133007

CONFIDENTIAL



ACTIVATE YOUR LIFELOCK MEMBERSHIP NOW.

Use this card when you visit **LifeLock.com** to take advantage of this very special member protection offer. LifeLock is available 24 hours a day, 7 days a week, 365 days a year to assist with your enrollment.

LifeLock

Relentlessly Protecting Your Identity

## Protect What Matters Most
## With LifeLock® Identity Theft Protection

LifeLock®
Relentlessly Protecting Your Identity®

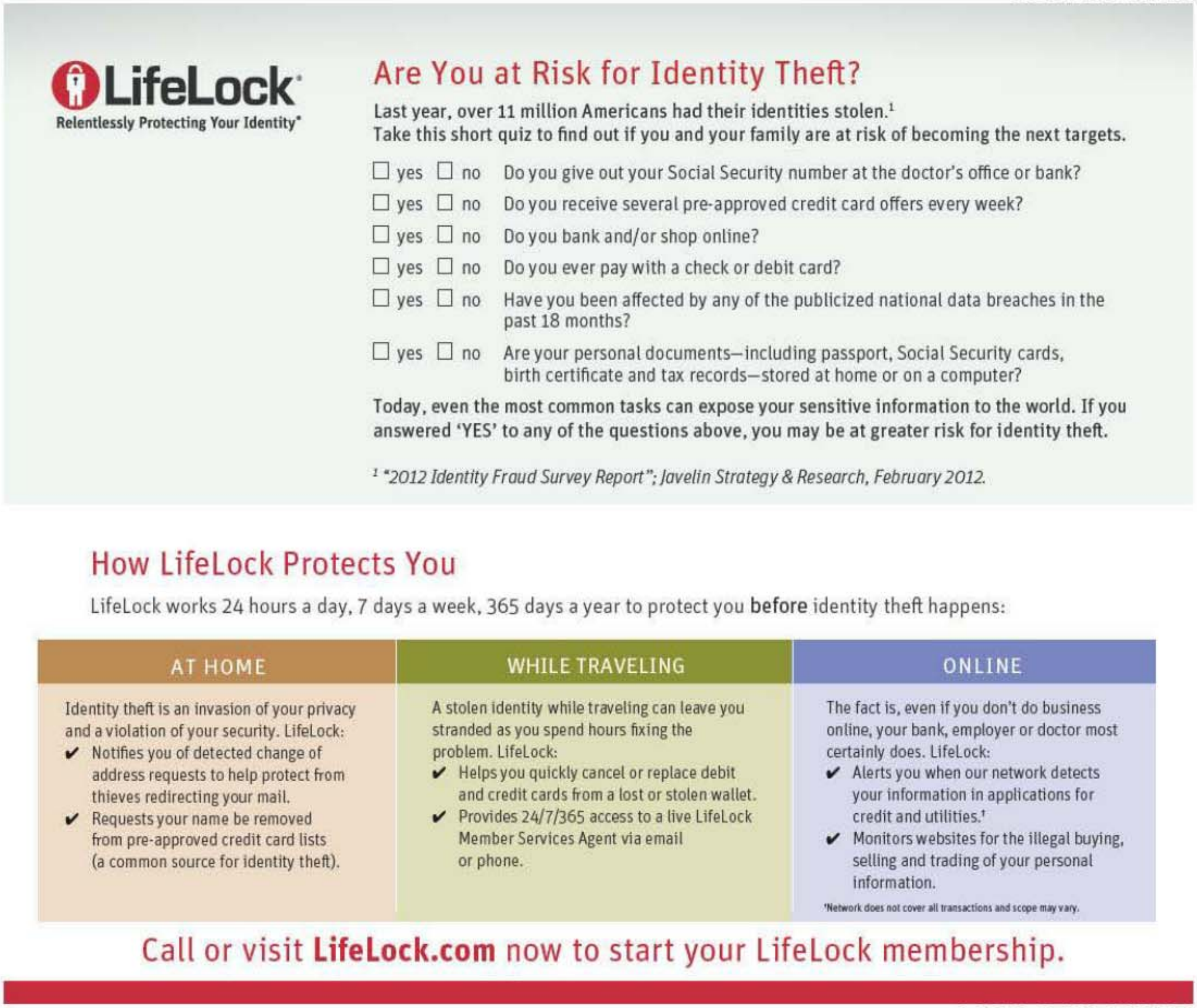
## Protect Your Identity Today.
## Start Your LifeLock® Membership Now.

Enrollment is quick and easy. Just use the enclosed enrollment card to take advantage of your special offer.

1. Call or visit LifeLock.com to start your identity theft protection today.
2. Provide the promotion code from your enrollment card.
3. Complete enrollment by providing your required information.

LifeLock®
Relentlessly Protecting Your Identity®

BROPC-0213



LifeLock
Relentlessly Protecting Your Identity®

## Are You at Risk for Identity Theft?

**Last year, over 11 million Americans had their identities stolen.[1]**
**Take this short quiz to find out if you and your family are at risk of becoming the next targets.**

- □ yes □ no Do you give out your Social Security number at the doctor's office or bank?
- □ yes □ no Do you receive several pre-approved credit card offers every week?
- □ yes □ no Do you bank and/or shop online?
- □ yes □ no Do you ever pay with a check or debit card?
- □ yes □ no Have you been affected by any of the publicized national data breaches in the past 18 months?
- □ yes □ no Are your personal documents—including passport, Social Security cards, birth certificate and tax records—stored at home or on a computer?

**Today, even the most common tasks can expose your sensitive information to the world. If you answered 'YES' to any of the questions above, you may be at greater risk for identity theft.**

[1] *"2012 Identity Fraud Survey Report"; Javelin Strategy & Research, February 2012.*

## How LifeLock Protects You

LifeLock works 24 hours a day, 7 days a week, 365 days a year to protect you **before** identity theft happens:

### AT HOME

Identity theft is an invasion of your privacy and a violation of your security. LifeLock:

- ✔ Notifies you of detected change of address requests to help protect from thieves redirecting your mail.
- ✔ Requests your name be removed from pre-approved credit card lists (a common source for identity theft).

### WHILE TRAVELING

A stolen identity while traveling can leave you stranded as you spend hours fixing the problem. LifeLock:

- ✔ Helps you quickly cancel or replace debit and credit cards from a lost or stolen wallet.
- ✔ Provides 24/7/365 access to a live LifeLock Member Services Agent via email or phone.

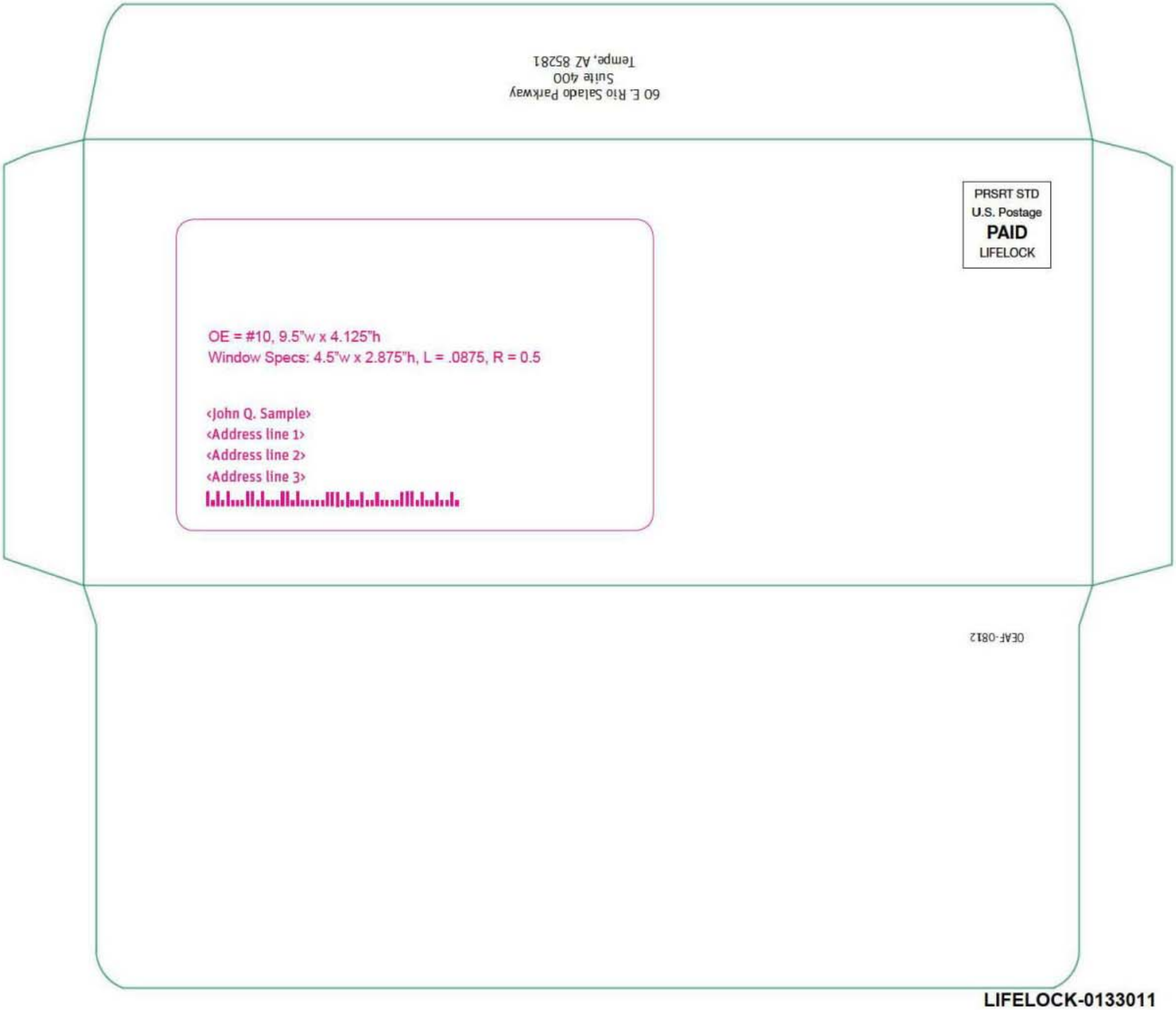
### ONLINE

The fact is, even if you don't do business online, your bank, employer or doctor most certainly does. LifeLock:

- ✔ Alerts you when our network detects your information in applications for credit and utilities.†
- ✔ Monitors websites for the illegal buying, selling and trading of your personal information.

†Network does not cover all transactions and scope may vary.

Call or visit **LifeLock.com** now to start your LifeLock membership.



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

PRSRT STD
U.S. Postage
**PAID**
LIFELOCK

OE = #10, 9.5"w x 4.125"h
Window Specs: 4.5"w x 2.875"h, L = .0875, R = 0.5

<John Q. Sample>
<Address line 1>
<Address line 2>
<Address line 3>

OEAF-0812

LifeLock®

CHOICEprivileges®
REWARDS PROGRAM

Benefit information enclosed for members of Choice Privileges.

ACTION REQUESTED by June 1, 2013—and use promo code CHOICEDM3!

**Special Offer for**
**Members of Choice Privileges:**
**30 Days FREE***
**+ 10% OFF = $9/MONTH**
**LIFELOCK IDENTITY THEFT PROTECTION**
**AND**
**Earn up to 4,500**
**Choice Privileges points****

‹John Q. Sample›
‹Address line 1›
‹Address line 2›
‹Address line 3›
‹Bar Code›

## Membership Activation Notice

Toll-Free Activation Hotline: **1-800-518-7902** or visit **LifeLock.com**
**NEW MEMBER OFFER: FREE for 30 Days*** when you activate before the deadline.
Your unique promo code: **CHOICEDM3** Act before: **June 1, 2013**

*At the end of the first 30 days, your card will be billed automatically ($9mo/$99yr plus applicable sales tax for standard LifeLock membership) unless you cancel within the 30-day trial period. You can cancel anytime without penalty by calling 1-800-LifeLock. Offer is for new LifeLock members only.

‹Dear John Q. Sample:›

Three seconds. That's the time it takes for another unsuspecting American to become a casualty of identity theft, a crime that victimized nearly one in twenty U.S. adults in 2011.[1]

Ten years ago you didn't hear much about identity theft. Nowadays, common tasks like sending an email or shopping online can leave you, your credit and your finances vulnerable to attack.

That is why I am pleased to introduce you to an exciting offer for members of **Choice Privileges** that works 24/7/365 to defend you from identity theft before it happens: **LifeLock® identity theft protection.**

The sophisticated technology from LifeLock works tirelessly to help protect you both online and offline by:

- Alerting you when your information is detected in applications for utility, cell phone and credit card accounts within the extensive LifeLock network.†
- Patrolling criminal Internet sites for the illegal buying, selling or trading of your personal information.
- Assisting you in canceling and replacing lost or stolen credit cards to help stop fraudulent charges.

While no one can prevent it entirely, LifeLock protects against many of the most serious types of identity theft.† And if LifeLock doesn't protect your identity, we will spend up to $1,000,000 to hire experts, lawyers and whomever else necessary to help your recovery.‡

**Act now and receive a SPECIAL CHOICE PRIVILEGES OFFER of 10% OFF the regular price when you sign up for LifeLock identity theft protection membership before June 1, 2013.** Use promo code **CHOICEDM3** and you will also get your first 30 days of LifeLock membership **FREE*** and **earn up to 4,500 Choice Privileges points.**** After the first 30 days, you'll be billed automatically at the discounted price of just $9 a month or $99 a year plus applicable sales tax for standard membership—a savings of 10%—unless you cancel within the first 30 days by calling 1-800-LifeLock.

Identity theft is real and so are the consequences. Protect yourself with LifeLock service today.

Sincerely,

Todd Davis

Todd Davis, CEO, LifeLock

**P.S. In the time it takes you to read this sentence, another identity may be stolen.** Do not wait.
It only takes minutes to sign up, but act before June 1, 2013 to take part in this special offer.
Call 1-800-518-7902 or visit LifeLock.com now.

Protect your identity with LifeLock service today:

Proactive identity threat alerts

Advanced Internet threat detection

Lost or stolen wallet protection

Access to special identity theft Member Services Agents

And more!

Enroll Now:
1-800-518-7902
LifeLock.com

†Network does not cover all transactions and scope may vary.

‡The benefits under the Service Guarantee are provided under a Master Insurance Policy underwritten by State National Insurance Company. As this is only a summary please see the actual policy for applicable terms and restrictions at LifeLock.com.

**Must be an active LifeLock member for 31 days to earn Choice Privileges points. Please allow 6–8 weeks for Choice Privileges points to be credited to your account. Choice Privileges members will earn 2,500 Choice Privileges points for the first year of standard LifeLock identity theft protection and 1,000 Choice Privileges points for standard membership in each of years 2 and 3. Choice Privileges members will earn 3,500 Choice Privileges points for the first year of LifeLock Ultimate™ enrollment and 1,250 Choice Privileges points for LifeLock Ultimate membership in each of years 2 and 3. Choice Privileges membership, earning of Choice Privileges points and redemption of Choice Privileges points are subject to Choice Privileges terms and conditions. Choice Privileges is owned by Choice Hotels International, Inc. Choice Hotels International is not affiliated with LifeLock.

[1] "2012 Identity Fraud Survey Report"; Javelin Strategy & Research, February 2012.

LifeLock
Relentlessly Protecting Your Identity®

**Choice Privileges Member:** **<John Q. Sample>**

Read what LifeLock members say.

Then call **1-800-518-7902** or visit **LifeLock.com** for **30 Days FREE*** **+ 10% OFF and earn up to 4,500 Choice Privileges points.****

## Real LifeLock Members
## SHARE THEIR STORIES:

*"LifeLock's protection has made me feel very safe about my identity—two incidents later and no damage."*

— LIFELOCK MEMBER, GENE Z.

*"When my identity was compromised, LifeLock caught it quickly. Within hours of the accounts opening, we had received the first call from LifeLock—which stopped any further problems."*

— LIFELOCK MEMBER, KRISTINA E.

*"I was a victim of identity theft, so I signed up for LifeLock. Six months later, I still was getting fraudulent applications, but LifeLock was catching all of them. Fortunately, in April 2010, it all stopped—and that's really because of LifeLock."*

— LIFELOCK MEMBER, JUSTIN L.

*"LifeLock saved me twice within the first five months of my enrollment."*

— LIFELOCK MEMBER, MICHELE C.

## QUICK QUIZ:

### IS LIFELOCK PROTECTION RIGHT FOR YOU?

YES NO

□ □ Do you pay for most purchases using a credit or debit card?

□ □ Have you ever misplaced your wallet?

□ □ Do you shop on the Internet?

□ □ Have any of your financial institutions suffered a data breach in the past 18 months?

□ □ Have you ever disposed of, donated or recycled an old computer?

□ □ Are your personal files—including passport and tax returns—stored in an unsecure place?

□ □ Do you dispose of mail without shredding it?

□ □ Is your mailbox unsecure or accessible to others besides your postal carrier?

□ □ Do you own a laptop computer?

□ □ Have you ever left your credit or debit card behind in a shop or restaurant?

□ □ Do you travel more than twice a year?

□ □ Are you using your home Internet service without an up-to-date firewall?

Even if you answered **YES** to just one of the above questions, please call LifeLock at 1-800-518-7902 to become a member right away.

LCTRL2-0113

## LifeLock® AWARD CERTIFICATE

CHOICEprivileges®
REWARDS PROGRAM

☑ **YES!** Please activate my LifeLock® membership to help protect my well-earned reputation—and hard-earned money. I understand that I can cancel within 30 days and owe nothing.* I also understand I'll receive 10% OFF the regular LifeLock membership rate if I decide to remain a member.

**Please act by June 1, 2013**
**and use promo code CHOICEDM3 to receive:**

**30 Days FREE***

**+ 10% OFF LifeLock Membership**

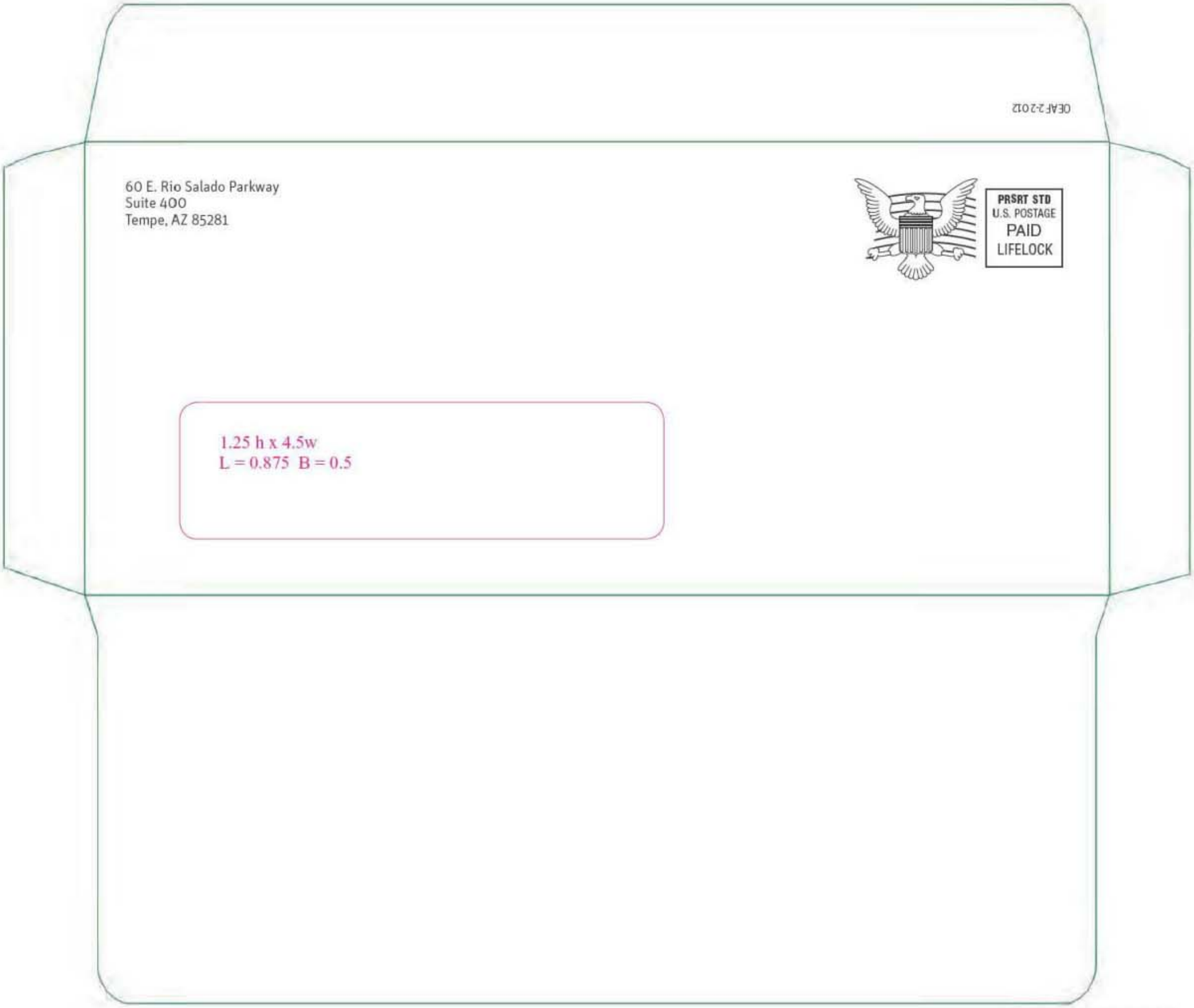
**and earn up to 4,500 Choice Privileges points****

**Activate your membership TODAY by calling 1-800-518-7902 or visit LifeLock.com**

*At the end of the first 30 days, your card will be billed automatically ($9mo/$99yr plus applicable sales tax for standard LifeLock membership) unless you cancel within the 30-day trial period. You can cancel anytime without penalty by calling 1-800-LifeLock. Offer is for new LifeLock members only.

**Must be an active LifeLock member for 31 days to earn Choice Privileges points. Please allow 6–8 weeks for Choice Privileges points to be credited to your account. Choice Privileges members will earn 2,500 Choice Privileges points for the first year of standard LifeLock identity theft protection and 1,000 Choice Privileges points for standard membership in each of years 2 and 3. Choice Privileges members will earn 3,500 Choice Privileges points for the first year of LifeLock Ultimate™ enrollment and 1,250 Choice Privileges points for LifeLock Ultimate membership in each of years 2 and 3. Choice Privileges membership, earning of Choice Privileges points and redemption of Choice Privileges points are subject to Choice Privileges terms and conditions. Choice Privileges is owned by Choice Hotels International, Inc. Choice Hotels International is not affiliated with LifeLock.

CONFIDENTIAL



**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF ARIZONA**

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

**LODGED UNDER SEAL**

**FTC PROPOSED EXHIBIT __11__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

BEST BUY | rewardzone

LifeLock®
Relentlessly Protecting Your Identity®

A. Gain Sample
8003 Franklin Farms Dr
Suite 200
Richmond, VA 23229
XXXXXXXXXXXXXXXXXXXXXXX

SPECIAL OFFER:

**30 Days FREE* + 10% OFF = $9/MONTH**
**and get up to 2,400 Reward Zone Points****

LIFELOCK IDENTITY THEFT PROTECTION

**that's nearly $50 in Best Buy rewards!**

Promotional code: **BBDM6B** Act before **October 1, 2013**

*At the end of the first 30 days, your card will be billed automatically ($9mo/$99yr plus applicable sales tax for standard LifeLock membership) unless you cancel within the 30-day trial period. You can cancel anytime without penalty by calling 1-800-LifeLock. Offer is for new LifeLock members only.

## MOST OF US THINK WE'RE THE LAST PERSON THAT WOULD EVER HAVE THEIR IDENTITY STOLEN...

Dear ‹A. Gain Sample›,

With over 12.6 million Americans having fallen victim to identity theft in 2012 alone,[1] it's all too common to hear stories of how this crime has had a lasting and detrimental impact on people's lives. We just don't think it can happen to us. **THAT'S WHY BEST BUY® REWARD ZONE® IS PROUD TO PARTNER WITH LIFELOCK® IDENTITY THEFT PROTECTION SERVICE WITH A FREE 30-DAY TRIAL PLUS 10% OFF* AND GET UP TO 2,400 REWARD ZONE POINTS.**** While no one can prevent all identity theft, LifeLock protects against many of the most serious types of identity theft.[†]

Here are some stories from actual victims. And they are from people just like you.

CASE FILE: 3672-86

**Name:** Justin L.

**Incident:** "I got a call from a credit card company saying, 'We want to verify this application that you applied for.' I said, 'I don't know who you are. I never applied for anything.' That started about a six month nightmare. I said enough is enough and signed up for LifeLock..."

**LifeLock member since 2009**

CASE FILE: 8154-21

**Name:** Michele C.

**Incident:** "Somebody got a copy of my driver's license and they went ahead and manufactured a bunch of false checks. They took them to a brand name store and cashed checks that were approved. A very good friend of mine said I should sign up for LifeLock..."

**LifeLock member since 2009**

CASE FILE: 2157-49

**Name:** Kristina E.

**Incident:** "I called LifeLock and said, 'This company is trying to get a hold of me, and they want to know why I have over $1,000 that I owe them. I've never opened an account with them.' LifeLock was so incredible, they took care of everything..."

**LifeLock member since 2009**

These are real members who allowed LifeLock to share their stories.

**PROTECT YOURSELF AND YOUR FAMILY AGAINST IDENTITY THEFT WITH LIFELOCK SERVICE TODAY, ALL WHILE EARNING REWARD ZONE POINTS.**

Unfortunately, identity theft is a real threat every day. So don't wait until you become another statistic, start protecting your vital personal information today. It takes just minutes to sign up—and then you can rest easy. Try LifeLock protection today and get it **FREE FOR 30 DAYS PLUS 10% OFF* AND GET UP TO 2,400 REWARD ZONE POINTS!****

Sincerely,

Bob Soukup, Senior Director, Loyalty, Best Buy, Inc.

## "IF I KNEW IT WAS THIS EASY, I WOULD HAVE SIGNED UP MONTHS AGO!"

**LIFELOCK IDENTITY THEFT PROTECTION**
**ONLY $9 A MONTH WITH THIS OFFER**

**$1 MILLION TOTAL SERVICE GUARANTEE[‡]**
If you become a victim of identity theft,
LifeLock will spend up to $1 million to hire experts to help your recovery.

Call **1-877-677-7999** or visit **LifeLock.com** today and get a 30-Day FREE Trial plus 10% OFF* and get up to 2,400 Reward Zone points.** Be sure to use promo code **BBDM6B** when signing up! Act before **October 1, 2013.**

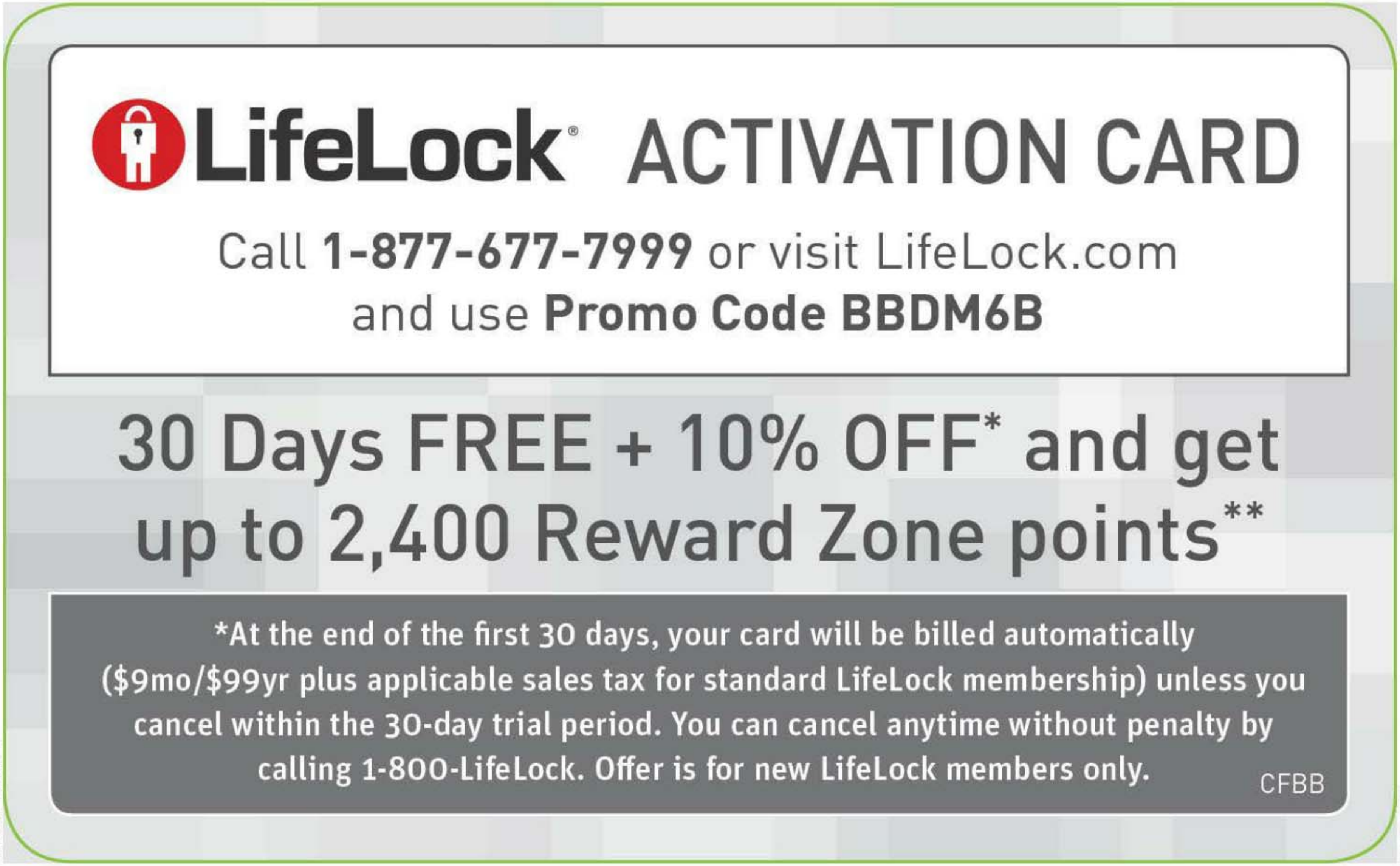
[†] Network does not cover all transactions and scope may vary.

[‡] The benefits under the Service Guarantee are provided under a Master Insurance Policy underwritten by State National Insurance Company. As this is only a summary please see the actual policy for applicable terms and restrictions at LifeLock.com.

**Annual LifeLock members will receive 2,000 points for the first year of LifeLock identity theft protection and 400 points for LifeLock membership in year two from Best Buy Reward Zone. Monthly LifeLock members will receive 500 points for their LifeLock enrollment. Reward Zone points shall be granted to the Reward Zone member in accordance with the terms and conditions of the Best Buy Reward Zone program available at MYRZ.com. Must be an active LifeLock member for 31 days after enrollment to be eligible for points. Offer is for new LifeLock members only. Please allow 6-8 weeks for points to post to your Reward Zone Account.

[1] "How Consumers can Protect Against Identity Fraudsters in 2013"; Javelin Strategy & Research, February 2013.

If you no longer wish to receive mail from Best Buy, please send a request, along with your name and mailing address to: Best Buy Corporate Campus, 7601 Penn Ave. S, Richfield, MN 55423-3645, ATTN: Customer Care/Privacy.



# LifeLock® ACTIVATION CARD

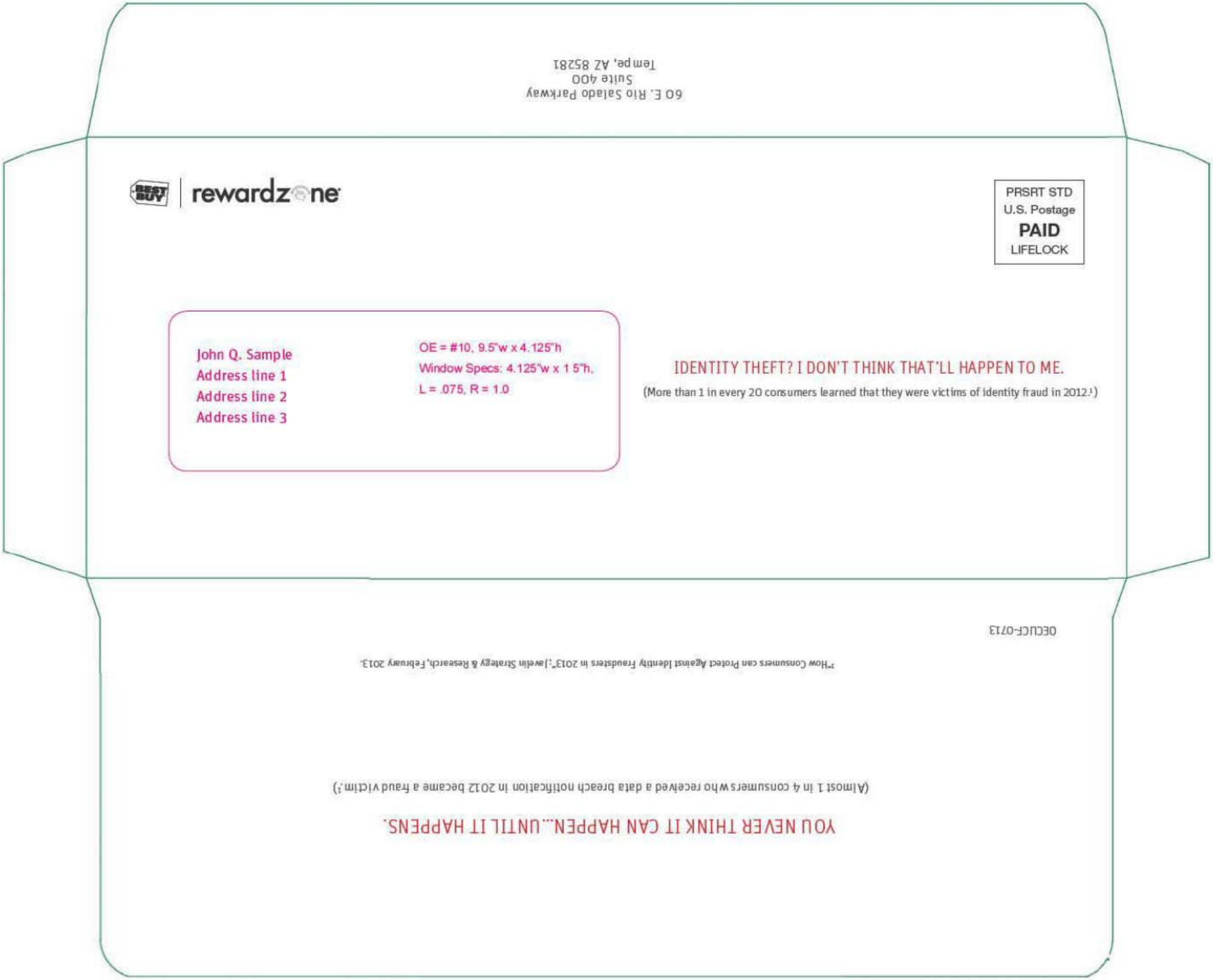
Call **1-877-677-7999** or visit LifeLock.com
and use **Promo Code BBDM6B**

## 30 Days FREE + 10% OFF* and get up to 2,400 Reward Zone points**

*At the end of the first 30 days, your card will be billed automatically ($9mo/$99yr plus applicable sales tax for standard LifeLock membership) unless you cancel within the 30-day trial period. You can cancel anytime without penalty by calling 1-800-LifeLock. Offer is for new LifeLock members only.

CFBB

**Annual LifeLock members will receive 2,000 points for the first year of LifeLock identity theft protection and 400 points for LifeLock membership in year two from Best Buy Reward Zone. Monthly LifeLock members will receive 500 points for their LifeLock enrollment. Reward Zone points shall be granted to the Reward Zone member in accordance with the terms and conditions of the Best Buy Reward Zone program available at MYRZ.com. Must be an active LifeLock member for 31 days after enrollment to be eligible for points. Offer is for new LifeLock members only. Please allow 6-8 weeks for points to post to your Reward Zone Account. If you no longer wish to receive mail from Best Buy, please send a request, along with your name and mailing address to: Best Buy Corporate Campus, 7601 Penn Ave. S, Richfield, MN 55423-3645, ATTN: Customer Care/Privacy.



PRSRT STD
U.S. Postage
**PAID**
LIFELOCK

John Q. Sample
Address line 1
Address line 2
Address line 3

OE = #10, 9.5"w x 4.125"h
Window Specs: 4.125"w x 1 5"h,
L = .075, R = 1.0

IDENTITY THEFT? I DON'T THINK THAT'LL HAPPEN TO ME.

(More than 1 in every 20 consumers learned that they were victims of identity fraud in 2012.[1])

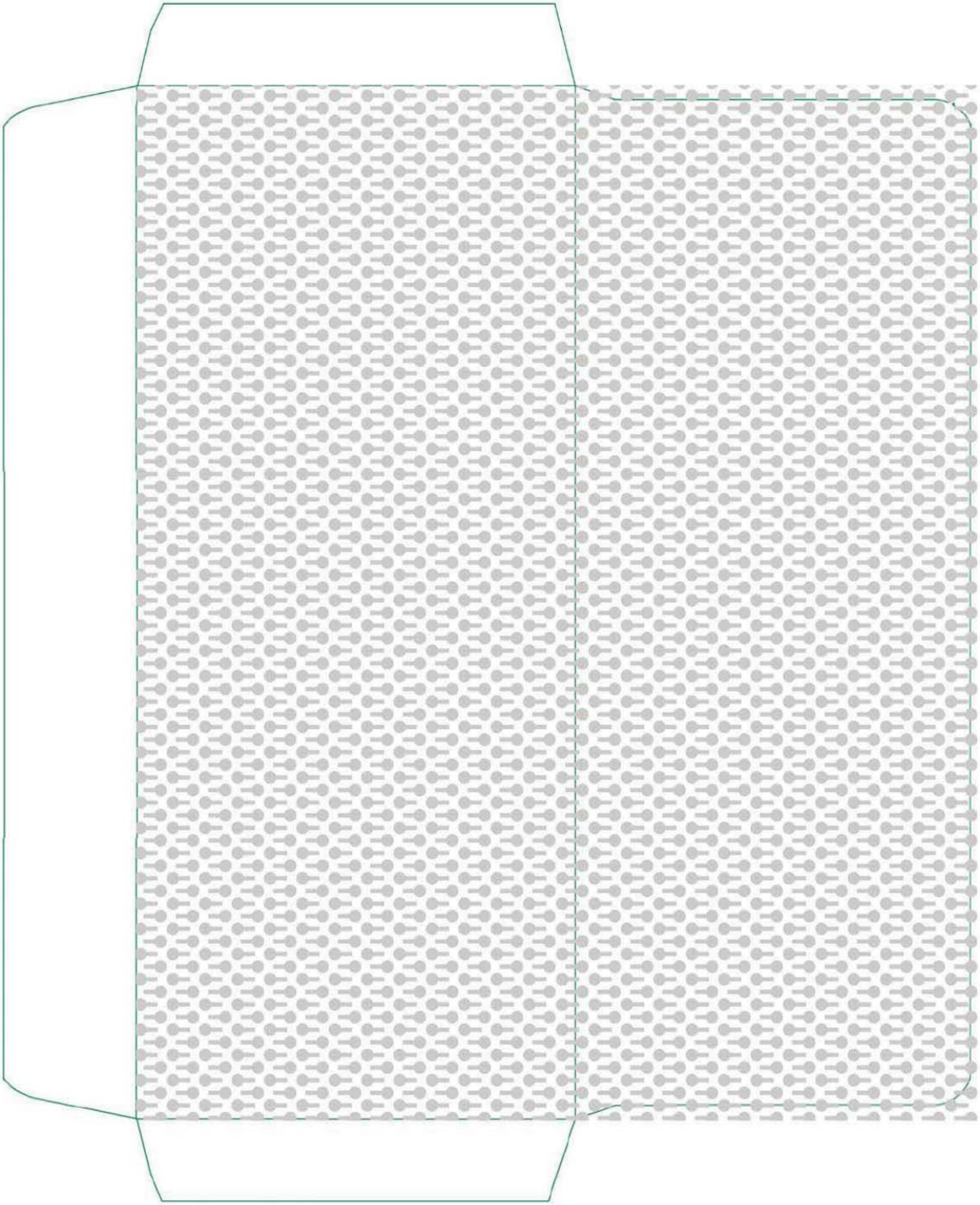
60 E. Rio Salado Parkway
Suite 400
Tempe, AZ 85281

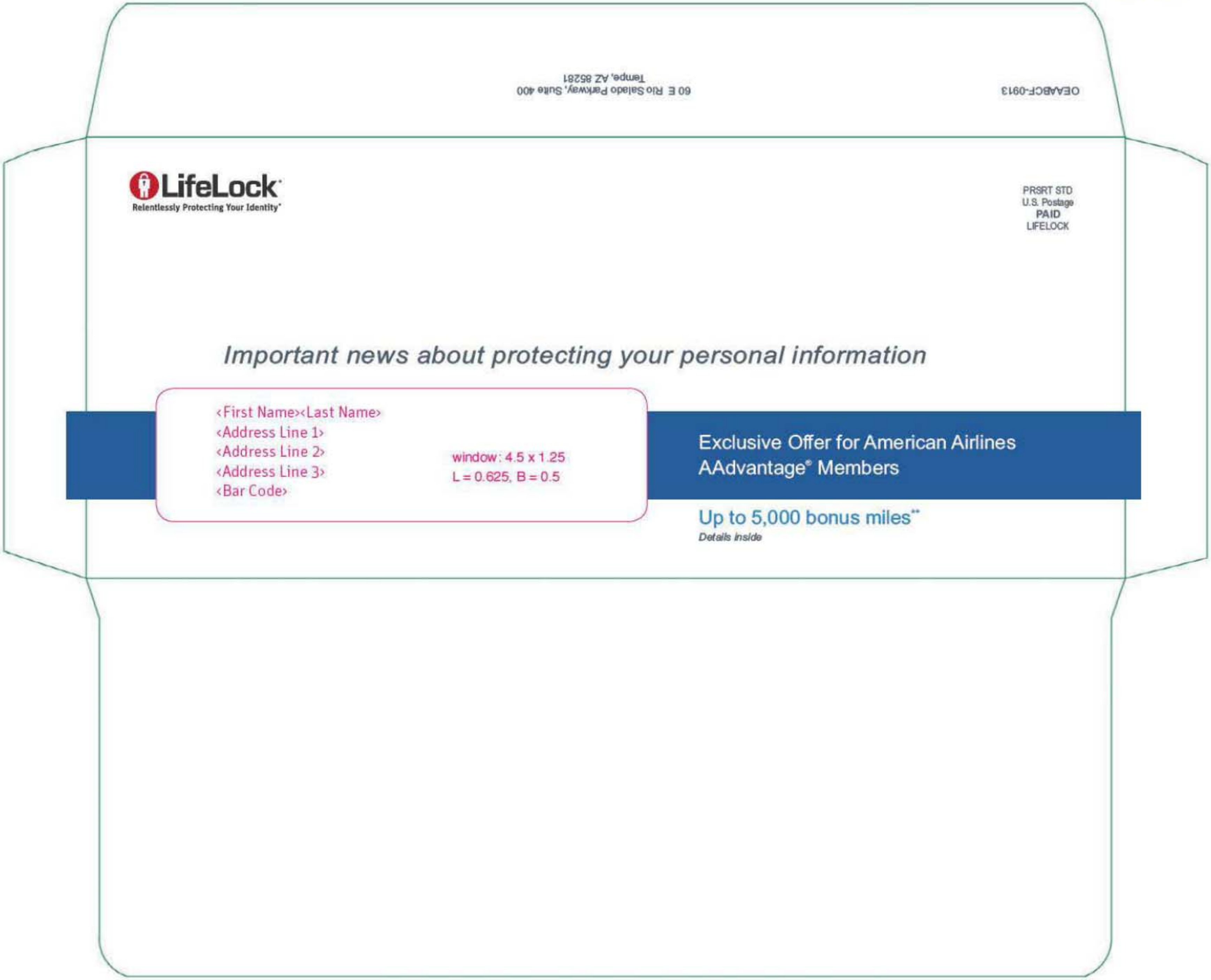
YOU NEVER THINK IT CAN HAPPEN...UNTIL IT HAPPENS.

(Almost 1 in 4 consumers who received a data breach notification in 2012 became a fraud victim.[1])

[1] "How Consumers can Protect Against Identity Fraudsters in 2013"; Javelin Strategy & Research, February 2013.

OECUCF-0713





OEAABCF-0913

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

LifeLock
Relentlessly Protecting Your Identity

PRSRT STD
U.S. Postage
PAID
LIFELOCK

*Important news about protecting your personal information*

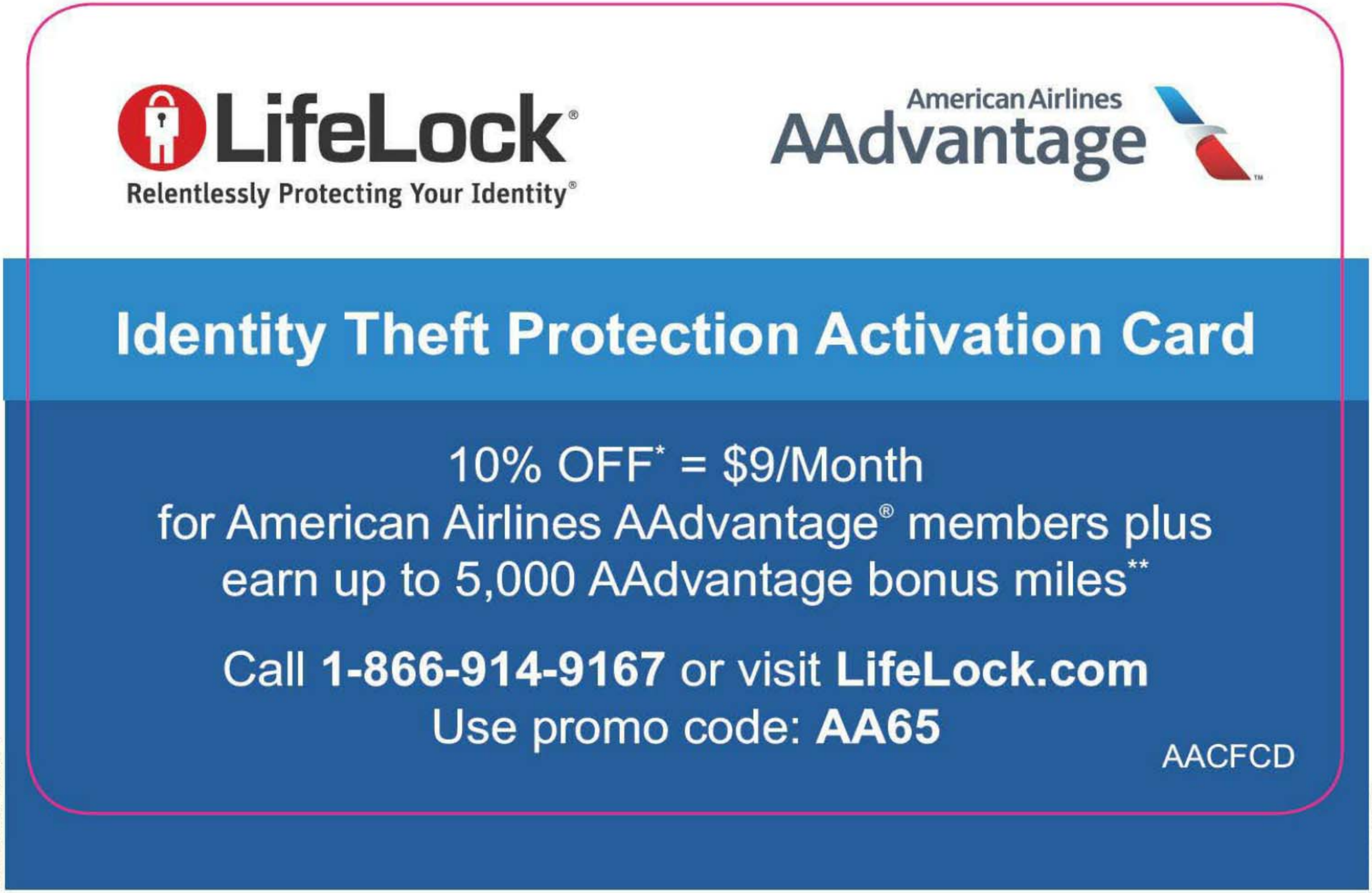
‹First Name›‹Last Name›
‹Address Line 1›
‹Address Line 2›
‹Address Line 3›
‹Bar Code›

window: 4.5 x 1.25
L = 0.625, B = 0.5

Exclusive Offer for American Airlines AAdvantage® Members

Up to 5,000 bonus miles**

*Details inside*



LifeLock®

Relentlessly Protecting Your Identity®

American Airlines AAdvantage™

## Identity Theft Protection Activation Card

10% OFF* = $9/Month
for American Airlines AAdvantage® members plus
earn up to 5,000 AAdvantage bonus miles**

Call **1-866-914-9167** or visit **LifeLock.com**
Use promo code: **AA65**

AACFCD

*Offer is for new LifeLock members only. Pricing refers to standard LifeLock identity theft protection only and does not include applicable sales tax. Members may cancel at any time without penalty by calling 1-800-LifeLock.

**See accompanying letter for AAdvantage® bonus miles terms.

LifeLock
Relentlessly Protecting Your Identity®

American Airlines
AAdvantage

*Up to 5,000 AAdvantage bonus miles** reserved for:*

<First Name><Last Name>
<Address Line 1>
<Address Line 2>
<Address Line 3>
<Bar Code>

**10% OFF* = $9/Month**
**for American Airlines AAdvantage Members plus earn up to 5,000 AAdvantage bonus miles****

Call **1-866-914-9167**
or visit **LifeLock.com**

Use promo code: **AA65**

*See next page for offer details*

Dear <First Name><Last Name>,

From neighborhood stores and restaurants to healthcare providers and employers, you leave a trail of personal information practically everywhere you go. Helping make sure that information stays personal has never been more important.

That's why LifeLock is proud to bring valued American Airlines AAdvantage® members like you this exclusive offer: **10% OFF* LifeLock® identity theft protection—and up to 5,000 AAdvantage bonus miles.****

Here are some stories from actual LifeLock members. And they are from people just like you.

CASE FILE: 3672-86

**Name:** Justin L.

**Incident:** "I got a call from a credit card company saying, 'We want to verify this application that you applied for.' I said, 'I don't know who you are. I never applied for anything.' That started about a six month nightmare. I said enough is enough and signed up for LifeLock..."

**LifeLock member since 2009**

CASE FILE: 8154-21

**Name:** Michele C.

**Incident:** "Somebody got a copy of my driver's license and they went ahead and manufactured a bunch of false checks. They took them to a brand name store and cashed checks that were approved. A very good friend of mine said I should sign up for LifeLock..."

**LifeLock member since 2009**

CASE FILE: 2157-49

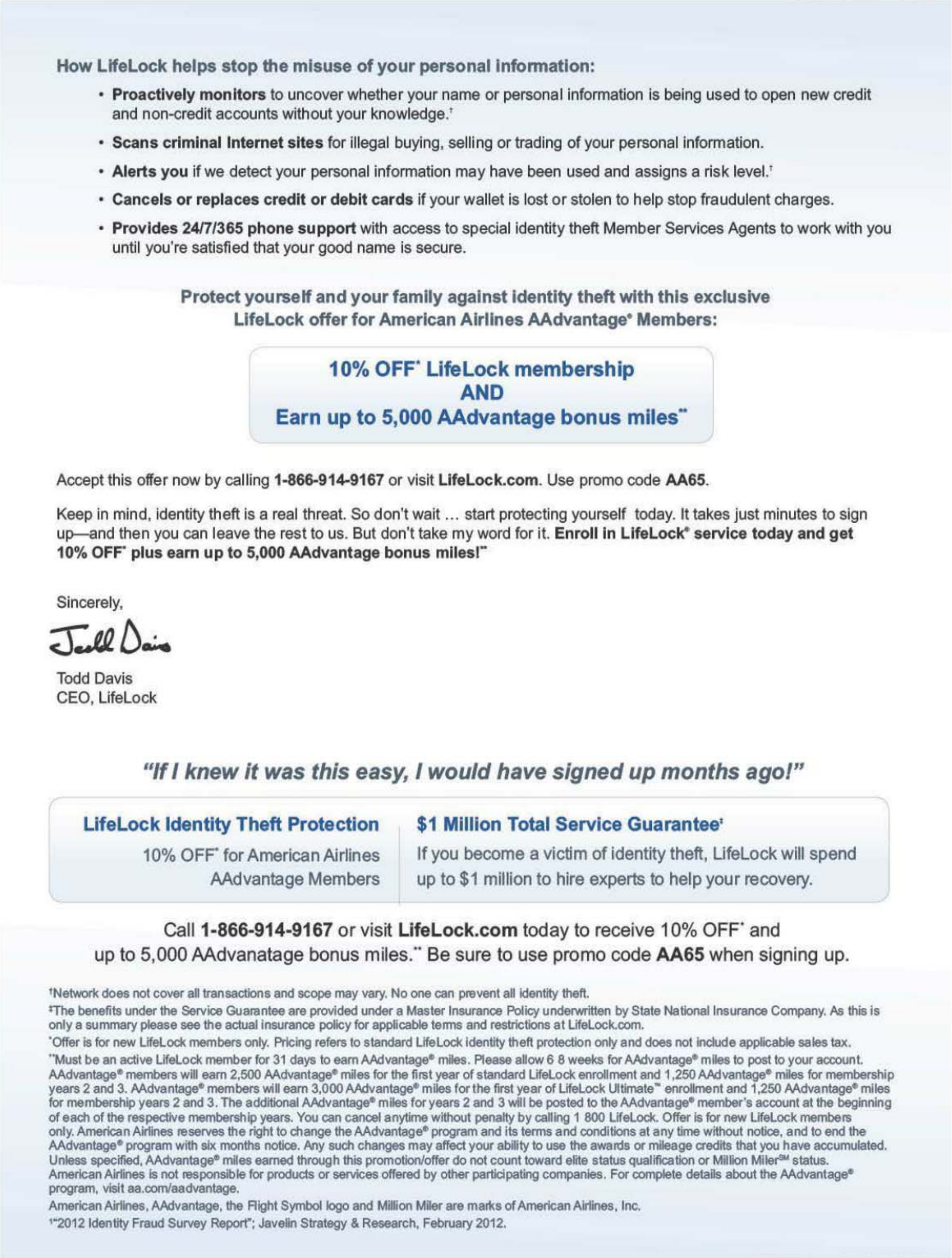
**Name:** Kristina E.

**Incident:** "I called LifeLock and said, 'This company is trying to get a hold of me, and they want to know why I have over $1,000 that I owe them. I've never opened an account with them.' LifeLock was so incredible, they took care of everything..."

**LifeLock member since 2009**

These are real members who have allowed LifeLock to share their stories.
If you would like to read additional member stories or learn more details, visit LifeLock.com.

*over, please*



**How LifeLock helps stop the misuse of your personal information:**

- **Proactively monitors** to uncover whether your name or personal information is being used to open new credit and non-credit accounts without your knowledge.[†]
- **Scans criminal Internet sites** for illegal buying, selling or trading of your personal information.
- **Alerts you** if we detect your personal information may have been used and assigns a risk level.[†]
- **Cancels or replaces credit or debit cards** if your wallet is lost or stolen to help stop fraudulent charges.
- **Provides 24/7/365 phone support** with access to special identity theft Member Services Agents to work with you until you're satisfied that your good name is secure.

**Protect yourself and your family against identity theft with this exclusive LifeLock offer for American Airlines AAdvantage® Members:**

**10% OFF[*] LifeLock membership**
**AND**
**Earn up to 5,000 AAdvantage bonus miles[**]**

Accept this offer now by calling **1-866-914-9167** or visit **LifeLock.com**. Use promo code **AA65**.

Keep in mind, identity theft is a real threat. So don't wait ... start protecting yourself today. It takes just minutes to sign up—and then you can leave the rest to us. But don't take my word for it. **Enroll in LifeLock® service today and get 10% OFF[*] plus earn up to 5,000 AAdvantage bonus miles![**]**

Sincerely,

Todd Davis

Todd Davis
CEO, LifeLock

***"If I knew it was this easy, I would have signed up months ago!"***

**LifeLock Identity Theft Protection**

10% OFF[*] for American Airlines AAdvantage Members

**$1 Million Total Service Guarantee[‡]**

If you become a victim of identity theft, LifeLock will spend up to $1 million to hire experts to help your recovery.

Call **1-866-914-9167** or visit **LifeLock.com** today to receive 10% OFF[*] and up to 5,000 AAdvanatage bonus miles.[**] Be sure to use promo code **AA65** when signing up.

[†] Network does not cover all transactions and scope may vary. No one can prevent all identity theft.

[‡] The benefits under the Service Guarantee are provided under a Master Insurance Policy underwritten by State National Insurance Company. As this is only a summary please see the actual insurance policy for applicable terms and restrictions at LifeLock.com.

[*] Offer is for new LifeLock members only. Pricing refers to standard LifeLock identity theft protection only and does not include applicable sales tax.

[**] Must be an active LifeLock member for 31 days to earn AAdvantage® miles. Please allow 6 8 weeks for AAdvantage® miles to post to your account. AAdvantage® members will earn 2,500 AAdvantage® miles for the first year of standard LifeLock enrollment and 1,250 AAdvantage® miles for membership years 2 and 3. AAdvantage® members will earn 3,000 AAdvantage® miles for the first year of LifeLock Ultimate™ enrollment and 1,250 AAdvantage® miles for membership years 2 and 3. The additional AAdvantage® miles for years 2 and 3 will be posted to the AAdvantage® member's account at the beginning of each of the respective membership years. You can cancel anytime without penalty by calling 1 800 LifeLock. Offer is for new LifeLock members only. American Airlines reserves the right to change the AAdvantage® program and its terms and conditions at any time without notice, and to end the AAdvantage® program with six months notice. Any such changes may affect your ability to use the awards or mileage credits that you have accumulated. Unless specified, AAdvantage® miles earned through this promotion/offer do not count toward elite status qualification or Million Miler℠ status. American Airlines is not responsible for products or services offered by other participating companies. For complete details about the AAdvantage® program, visit aa.com/aadvantage.

American Airlines, AAdvantage, the Flight Symbol logo and Million Miler are marks of American Airlines, Inc.

[1] "2012 Identity Fraud Survey Report"; Javelin Strategy & Research, February 2012.

# MEMBER BENEFIT NOTIFICATION

<First Name><Last Name>

**Simply call toll-free 1-800-982-5114 or visit LifeLock.com and use promo code NRAMAIL6 to activate your LifeLock Identity Theft Protection with a 60-Day Money Back Guarantee* plus a 10% lifetime discount for as long as you remain a member!**

Dear <FirstName><LastName>,

In the time it takes you to read this sentence, a thief could gain access to your personal information to commit crimes of identity fraud.

In fact, more than 1 in every 20 US adults learned they were victims of identity theft in 2013.[1] The problem is growing so rapidly, and the damage—to your finances and to your reputation—can be so severe, the NRA has taken steps to help members protect themselves.

> With that in mind, I'm pleased to announce that NRA members will get a 60-Day Money Back Guarantee* plus you'll save 10% on LifeLock® identity theft protection membership—America's leader in the industry. Your 10% savings will be honored as long as you choose to maintain your LifeLock membership. That's just $9 a month!*
>
> Call **1-800-982-5114** or visit **LifeLock.com**, to get started.
> Be sure to refer to Promo Code **NRAMAIL6**.

Once you've enrolled, you'll receive LifeLock identity theft protection with a 60-Day Money Back Guarantee.* With your LifeLock membership, you will receive these benefits:

1. **Identity Alerts**—an "early warning system" that alerts you of potential misuse of your personal information detected in the network.†
2. **Advanced Internet Monitoring**—which monitors over 10,000 black market websites where stolen personal account and identification numbers are bought and sold.
3. **Lost Wallet Protection**—which replaces not only credit cards but also driver's licenses and other official documents if your wallet is ever lost or stolen. (Excludes pictures, cash and cash equivalents.)
4. **$1,000,000 Total Service Guarantee**—If you become a victim of identity theft, LifeLock will spend up to $1,000,000 to hire experts to help your recovery.‡

**As a NRA member, you'll SAVE 10% on LifeLock service for the life of your membership.
BUT YOU MUST ENROLL NOW.**

It's alarming, but true: your personal identity may potentially be at risk every time you use a credit card, every time you use a debit card, every time you use an ATM or every time you make an online transaction. Identity thieves have high-tech devices at their disposal that can literally snatch personal

(over, please)

*If you are not satisfied with LifeLock service, simply call 1-800-LifeLock to cancel your membership within the first 60 days to receive a complete refund of your purchase price. Offer is for new LifeLock members only. Pricing refers to standard LifeLock identity theft protection only and does not include applicable sales tax.

†Network does not cover all transactions and scope may vary.

‡The benefits under the Service Guarantee are provided under a Master Insurance Policy underwritten by State National Insurance Company. As this is only a summary please see the actual policy for applicable terms and restrictions at LifeLock.com.

No NRA Member dues or contributions are used for this program, promotion or any other related expenses.

LTRNRASB0114

Slit/area

## LifeLock Service Statement of Benefits

317

Prepared for NRA Member <First Name><Last Name>

| Program:<br>LifeLock® Identity Theft Protection | Benefit:<br>60-Day Money Back Guarantee*<br>plus a 10% discount. | Action Needed:<br>Call 1-800-982-5114 or visit LifeLock.com. | Refer to Promo Code:<br>NRAMAIL6 |
|---|---|---|---|
| **Benefit Title** | | **Description** | **Status** |
| ✓ **Identity Alerts** | | Thieves can do damage if they get their hands on personal information like your Social Security number. LifeLock proactively monitors your personal information and alerts you to potential threats within the network—both credit and noncredit related, so you can act before they become really big problems.† | **INCLUDED** |
| ✓ **Advanced Internet Monitoring** | | When your personal information falls into the wrong hands, it may end up on one or more of the thousands of black market information exchange sites where stolen personal account and identification numbers are bought and sold. LifeLock monitors these sites to see if your information is up for sale. | **INCLUDED** |
| ✓ **Lost Wallet Protection** | | If your wallet is lost or stolen, how much time would it take you to replace all the cards and important documents you carry...If you could even remember them all? LifeLock will take care of canceling and replacing all your credit, debit and bank cards. And they'll even help you replace official documents like driver's licenses! (Excludes pictures, cash and cash equivalents.) | **INCLUDED** |
| ✓ **$1,000,000 Total Service Guarantee** | | If you become a victim of identity theft, LifeLock will spend up to $1,000,000 to hire experts to help your recovery.‡ | **INCLUDED** |
| ✓ **Personalized Online Dashboard** | | You'll have 24/7 online access to a personalized dashboard showing current threats within the network. | **INCLUDED** |

**As a NRA member, you get 60-Day Money Back Guarantee* plus a 10% discount for the lifetime of your LifeLock membership! BUT YOU MUST ENROLL.
Call 1-800-982-5114 or visit LifeLock.com and refer to the promo code above.**

*If you are not satisfied with LifeLock service, simply call 1-800-LifeLock to cancel your membership within the first 60 days to receive a complete refund of your purchase price. Offer is for new LifeLock members only. Pricing refers to standard LifeLock identity theft protection only and does not include applicable sales tax.

†Network does not cover all transactions and scope may vary.

‡The benefits under the Service Guarantee are provided under a Master Insurance Policy underwritten by State National Insurance Company. As this is only a summary please see the actual policy for applicable terms and restrictions at LifeLock.com.

No NRA Member dues or contributions are used for this program, promotion or any other related expenses.

LifeLock®
Relentlessly Protecting Your Identity®

information from wireless Internet networks. They can hack your computer, or ransack your mailbox. And once they get their hands on your Social Security number, they can cause damage that could take you years to repair, or steal money that has taken you years to save.

I urge you to call 1-800-982-5114 right away to take advantage of this NRA member discount.

Sincerely,

Wilson H Phillips Jr.
Treasurer & CFO, National Rifle Association

P.S. The next time you take out your credit card could be the time your identity gets stolen. Don't wait. Start your LifeLock membership immediately with and receive a 60-Day Money Back Guarantee* plus a 10% discount for the life of your membership. Call today to enroll: 1-800-982-5114.

*If you are not satisfied with LifeLock service, simply call 1-800-LifeLock to cancel your membership within the first 60 days to receive a complete refund of your purchase price. Offer is for new LifeLock members only. Pricing refers to standard LifeLock identity theft protection only and does not include applicable sales tax.

†Network does not cover all transactions and scope may vary.

‡The benefits under the Service Guarantee are provided under a Master Insurance Policy underwritten by State National Insurance Company. As this is only a summary please see the actual policy for applicable terms and restrictions at LifeLock.com.

1. Q3 2013; Identity Theft Tracking Study; a commissioned survey conducted July–August by Forrester Consulting on behalf of LifeLock.

No NRA Member dues or contributions are used for this program, promotion or any other related expenses.

## Should I Enroll in Identity Theft Protection?

*Ask yourself these questions:*

*1.* Do you pay for most purchases using a credit or debit card? .................. □ Yes □ No

*2.* Do you shop online? .................. □ Yes □ No

*3.* Have you ever thrown out, recycled or donated an old computer? .................. □ Yes □ No

*4.* Are your personal documents—including passports, Social Security cards, birth certificates and tax records—stored in an unsecure place? .................. □ Yes □ No

*5.* Do you dispose of mail without shredding it? .................. □ Yes □ No

*6.* Is your mailbox unsecured or accessible to anyone other than your postal carrier? .................. □ Yes □ No

*7.* Have you been affected by any of the publicized national breaches in the past 18 months? □ Yes □ No

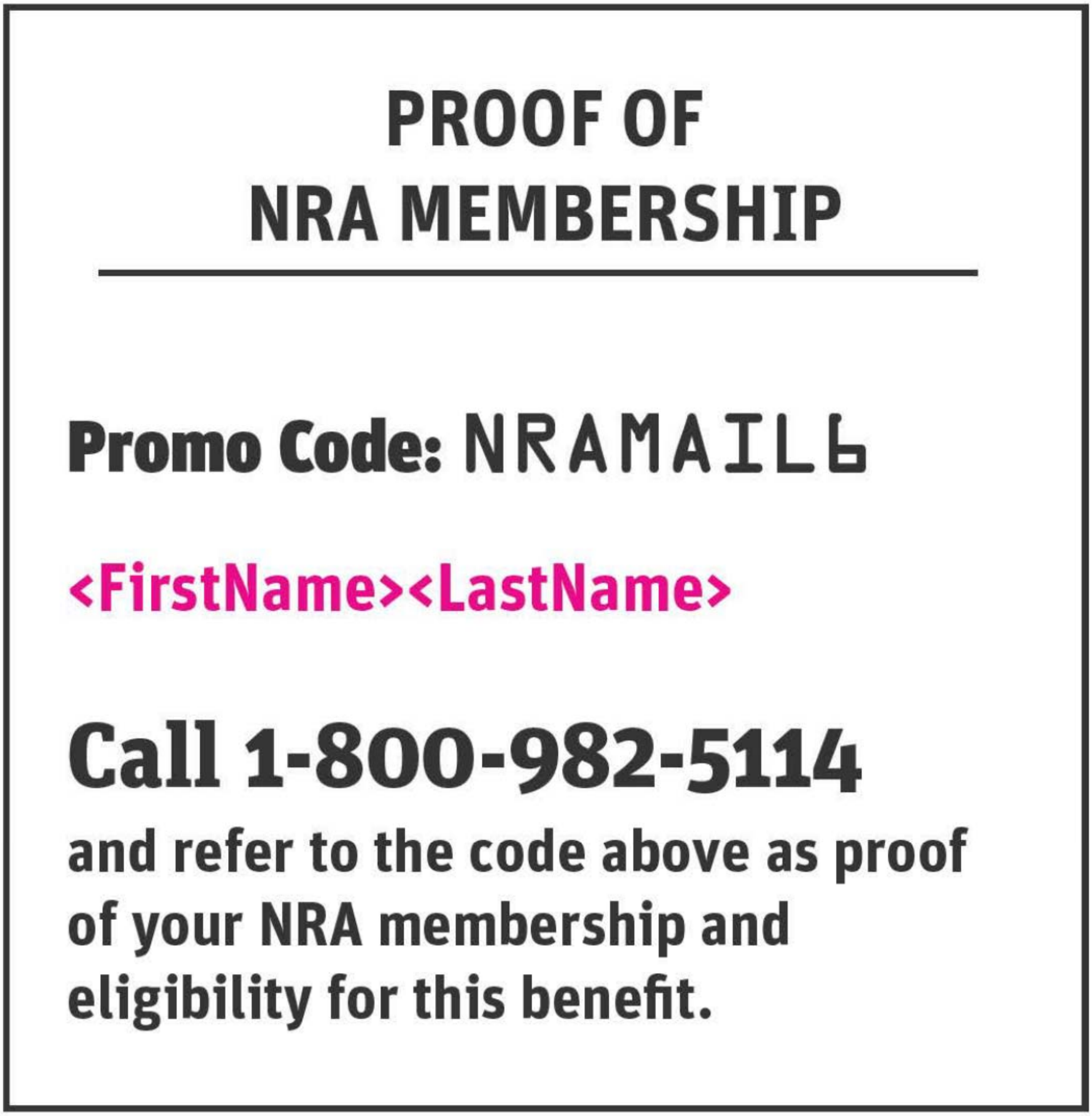
*8.* Are you using your home Internet service without an up-to-date firewall? .................. □ Yes □ No

*9.* Before leaving a restaurant, do you sometimes forget to make sure a bill you've paid by credit or debit card has been picked up by an employee? .................. □ Yes □ No

*10.* Have you ever accidentally left a credit or debit card behind in a shop or restaurant? .................. □ Yes □ No

**If you answered "Yes" to even one of these questions, activate your identity theft protection today...and SAVE 10% on your LifeLock membership for life!**

Slit/area



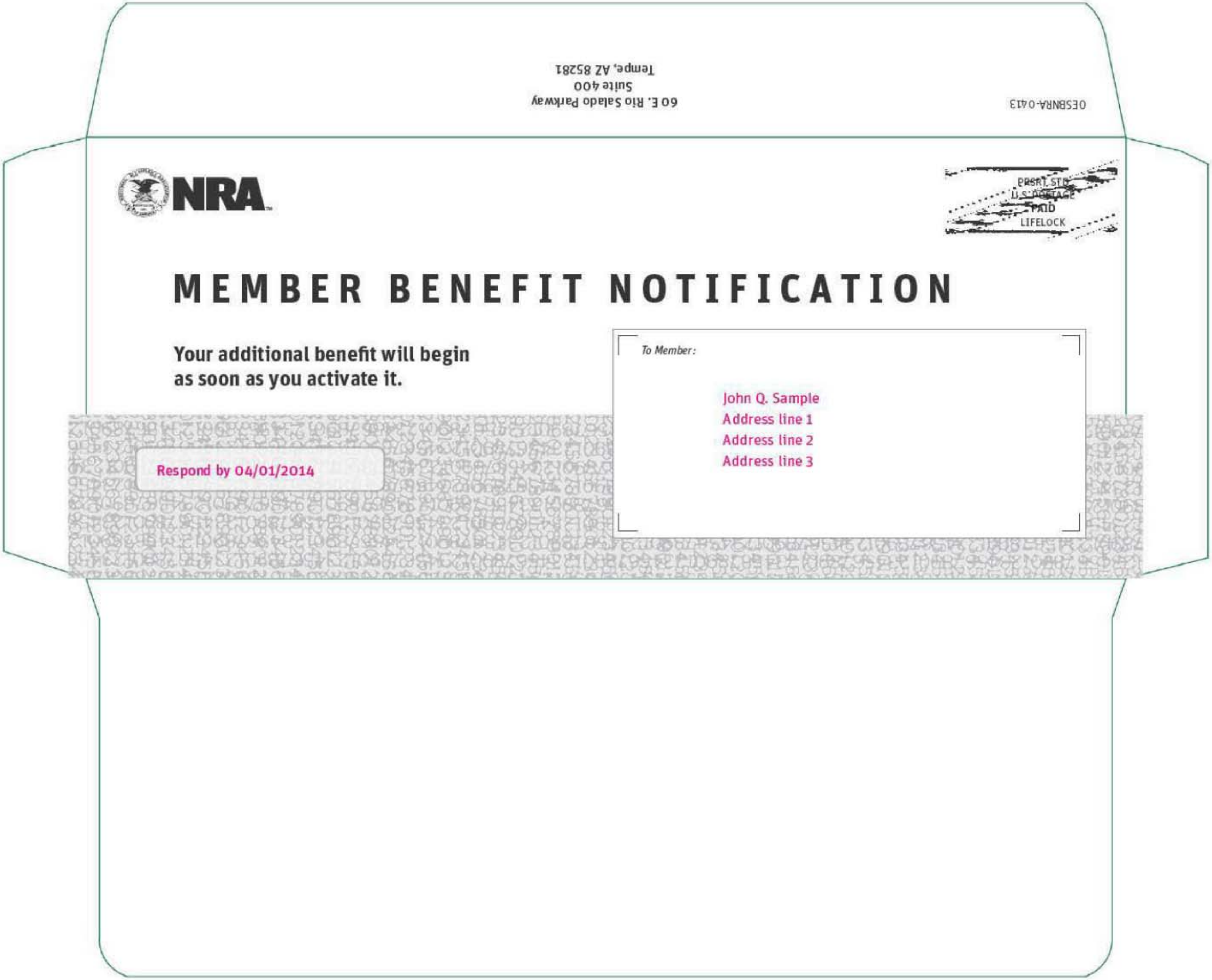
# PROOF OF NRA MEMBERSHIP

**Promo Code:** NRAMAIL6

<FirstName><LastName>

**Call 1-800-982-5114**

**and refer to the code above as proof of your NRA membership and eligibility for this benefit.**



OESBNRA-0413

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

PRSRT STD
U.S. POSTAGE
PAID
LIFELOCK

NRA

MEMBER BENEFIT NOTIFICATION

Your additional benefit will begin
as soon as you activate it.

Respond by 04/01/2014

*To Member:*

John Q. Sample
Address line 1
Address line 2
Address line 3

**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF ARIZONA**

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

**LODGED UNDER SEAL**

**FTC PROPOSED EXHIBIT __12__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

United States Patent and Trademark Office

Home | Site Index | Search | FAQ | Glossary | Guides | Contacts | eBusiness | eBiz alerts | News | Help

## Trademarks > Trademark Electronic Search System (TESS)

*TESS was last updated on Tue Sep 23 03:21:01 EDT 2014*

TESS HOME | NEW USER | STRUCTURED | FREE FORM | BROWSE DICT | SEARCH OG | BOTTOM | HELP

Logout Please logout when you are done to release system resources allocated for you.

## Record 1 out of 1

TSDR | ASSIGN Status | TTAB Status ***( Use the "Back" button of the Internet Browser to return to TESS)***

RELENTLESSLY PROTECTING
YOUR IDENTITY

| | |
|---|---|
| **Word Mark** | **RELENTLESSLY PROTECTING YOUR IDENTITY** |
| **Goods and Services** | IC 036. US 100 101 102. G & S: Providing credit reporting data maintained by others; credit risk management and consultation services in the field of identity theft, namely, assistance with restoring and analyzing credit damaged by identity theft; providing advice and consultation in the field of credit reports and credit scores in the context of identity theft; fraud resolution assistance, namely, assistance with restoring credit damaged by identity theft; and providing reimbursement of costs associated with identity theft. FIRST USE: 20100600. FIRST USE IN COMMERCE: 20100600<br>IC 045. US 100 101. G & S: Fraud detection and prevention services in the nature of arranging secure authentication of personal data in requests to open banking, credit, credit card, insurance, loan, and other financial accounts; Fraud and identity theft protection services; monitoring the Internet, public records, credit reports, private and public electronic databases, and unregulated global computer networks to facilitate the detection and prevention of identity theft and fraud; providing a secure interactive website concerning notifications of potential fraud and potential identity theft; resolution assistance, namely, providing advice and consultation in the field of data theft and identity theft; consultation in the field of data theft and identity theft; and tracking, monitoring, and reporting regarding consumer credit reports and changes thereto for purposes of protecting against data theft, identity theft and fraud. FIRST USE: 20100600. FIRST USE IN COMMERCE: 20100600 |
| **Standard Characters Claimed** | |
| **Mark Drawing Code** | (4) STANDARD CHARACTER MARK |
| **Serial Number** | 85095370 |
| **Filing Date** | July 28, 2010 |
| **Current Basis** | 1A |
| **Original Filing Basis** | 1B |

| | |
|---|---|
| **Published for Opposition** | January 18, 2011 |
| **Registration Number** | 4165114 |
| **Registration Date** | June 26, 2012 |
| **Owner** | (REGISTRANT) LifeLock, Inc. CORPORATION DELAWARE 60 E. Rio Salado Parkway Tempe ARIZONA 85281 |
| **Assignment Recorded** | ASSIGNMENT RECORDED |
| **Attorney of Record** | Heather A. Dunn, Esq. |
| **Prior Registrations** | 3604652;3780480 |
| **Type of Mark** | SERVICE MARK |
| **Register** | PRINCIPAL |
| **Live/Dead Indicator** | LIVE |

TESS HOME NEW USER STRUCTURED FREE FORM BROWSE DICT SEARCH OG TOP HELP

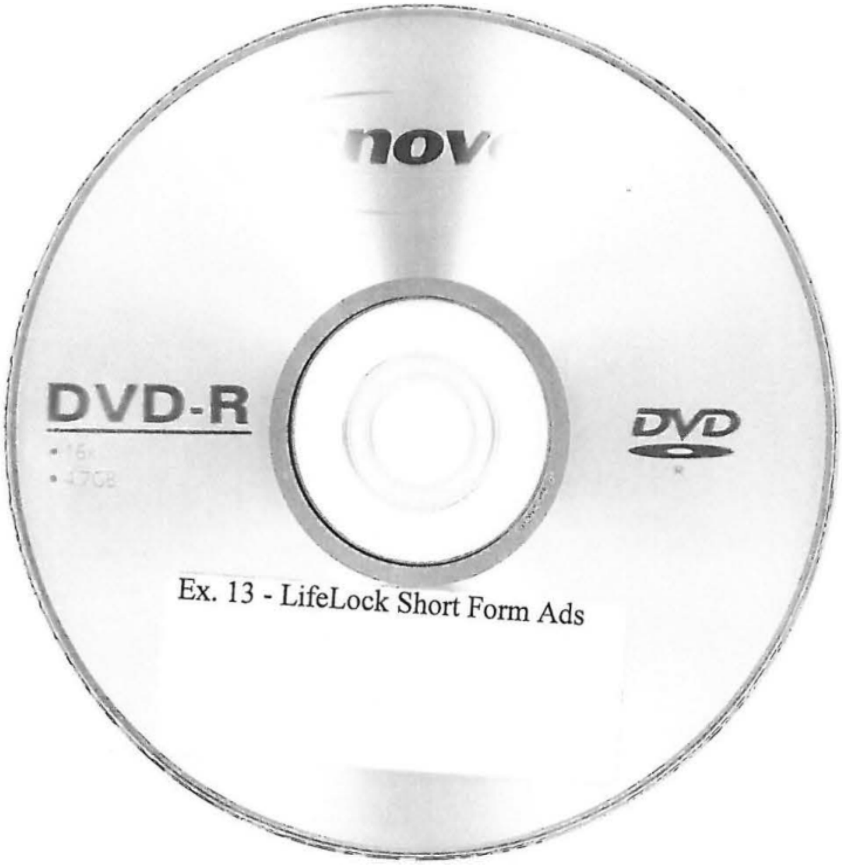
| .HOME | SITE INDEX | SEARCH | eBUSINESS | HELP | PRIVACY POLICY

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

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

**LODGED UNDER SEAL**

**FTC PROPOSED EXHIBIT __13__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**



Ex. 13 - LifeLock Short Form Ads

**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF ARIZONA**

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

**LODGED UNDER SEAL**

**FTC PROPOSED EXHIBIT __21__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

# Adobe Security Bulletin

## Security updates available for Adobe Flash Player

**Release date:** April 28, 2014

**Vulnerability identifier:** APSB14-13

**Priority:** See table below

**CVE number:** CVE-2014-0515

**Platform:** All Platforms

## Summary

Adobe has released security updates for Adobe Flash Player 13.0.0.182 and earlier versions for Windows, Adobe Flash Player 13.0.0.201 and earlier versions for Macintosh and Adobe Flash Player 11.2.202.350 and earlier versions for Linux. These updates address vulnerabilities that could potentially allow an attacker to take control of the affected system.

Adobe is aware of reports that an exploit for CVE-2014-0515 exists in the wild, and is being used to target Flash Player users on the Windows platform. Adobe recommends users update their product installations to the latest versions:

- Users of Adobe Flash Player 13.0.0.182 and earlier versions for Windows should update to Adobe Flash Player 13.0.0.206.
- Users of Adobe Flash Player 13.0.0.201 and earlier versions for Macintosh should update to Adobe Flash Player 13.0.0.206.
- Users of Adobe Flash Player 11.2.202.350 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.356.
- Adobe Flash Player 13.0.0.182 installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 13.0.0.206 for Windows, Macintosh and Linux.
- Adobe Flash Player 13.0.0.182 installed with Internet Explorer 10 will automatically be updated to the latest Internet Explorer 10 version, which will include Adobe Flash Player 13.0.0.206 for Windows 8.0.
- Adobe Flash Player 13.0.0.182 installed with Internet Explorer 11 will automatically be updated to the latest Internet Explorer 11 version, which will include Adobe Flash Player 13.0.0.206 for Windows 8.1.

## Affected software versions

- Adobe Flash Player 13.0.0.182 and earlier versions for Windows
- Adobe Flash Player 13.0.0.201 and earlier versions for Macintosh
- Adobe Flash Player 11.2.202.350 and earlier versions for Linux

To verify the version of Adobe Flash Player installed on your system, access the About Flash Player page, or right-click on content running in Flash Player and select "About Adobe (or Macromedia) Flash Player" from the menu. If you use multiple browsers, perform the check for each browser you have installed on your system.

## Solution

Adobe recommends users update their software installations by following the instructions below:

- Adobe recommends users of Adobe Flash Player 13.0.0.182 and earlier versions for Windows update to the newest version 13.0.0.206 by downloading it from the Adobe Flash Player Download Center, or via the update mechanism within the product when prompted.
- Adobe recommends users of Adobe Flash Player 13.0.0.201 and earlier versions for Macintosh update to the newest version 13.0.0.206 by downloading it from the Adobe Flash Player Download Center, or via the update mechanism within the product when prompted.
- Adobe recommends users of Adobe Flash Player 11.2.202.350 and earlier versions for Linux update to Adobe Flash Player 11.2.202.356 by downloading it from the Adobe Flash Player Download Center.
- For users of Flash Player 11.7.700.275 and earlier versions for Windows and Macintosh, who cannot update to Flash Player 13.0.0.206, Adobe has made available the update Flash Player 11.7.700.279*, which can be downloaded here.
- Adobe Flash Player 13.0.0.182 installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 13.0.0.206 for Windows, Macintosh and Linux.
- Adobe Flash Player 13.0.0.182 installed with Internet Explorer 10 will automatically be updated to the latest Internet Explorer 10 version, which will include Adobe Flash Player 13.0.0.206 for Windows 8.0.
- Adobe Flash Player 13.0.0.182 installed with Internet Explorer 11 will automatically be updated to the latest Internet Explorer 11 version, which will include Adobe Flash Player 13.0.0.206 for Windows 8.1.

* Beginning May 13, 2014, Adobe Flash Player 13 for Mac and Windows will replace version 11.7 as the extended support version. Adobe recommends users upgrade to version 13 to continue to receive security updates. See this blog post for further details http://blogs.adobe.com/flashplayer/2014/03/upcoming-changes-to-flash-players-extended-support-release.html

## Priority and severity ratings

Adobe categorizes these updates with the following priority ratings and recommends users update their installation to the newest version:

| Product | Updated version | Platform | Priority rating |
|---|---|---|---|
| Adobe Flash Player | 13.0.0.206 | Windows and Macintosh | 1 |
| | 13.0.0.206 | Internet Explorer 10 for Windows 8.0 | 1 |
| | 13.0.0.206 | Internet Explorer 11 for Windows 8.1 | 1 |

| | | |
|---|---|---|
| 13.0.0.206 | Chrome for Windows, Macintosh and Linux | 1 |
| 11.7.700.279 | Windows and Macintosh | 1 |
| 11.2.202.356 | Linux | 3 |

These updates address a critical vulnerability in the software.

## Details

Adobe has released security updates for Adobe Flash Player 13.0.0.182 and earlier versions for Windows, 13.0.0.201 and earlier versions for Macintosh and Adobe Flash Player 11.2.202.350 and earlier versions for Linux. These updates address vulnerabilities that could potentially allow an attacker to take control of the affected system. Adobe recommends users update their product installations to the latest versions:

- Users of Adobe Flash Player 13.0.0.182 and earlier versions for Windows should update to Adobe Flash Player 13.0.0.206.
- Users of Adobe Flash Player 13.0.0.201 and earlier versions for Macintosh should update to Adobe Flash Player 13.0.0.206.
- Users of Adobe Flash Player 11.2.202.350 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.356.
- Adobe Flash Player 13.0.0.182 installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 13.0.0.206 for Windows, Macintosh and Linux.
- Adobe Flash Player 13.0.0.182 installed with Internet Explorer 10 will automatically be updated to the latest Internet Explorer 10 version, which will include Adobe Flash Player 13.0.0.206 for Windows 8.0.
- Adobe Flash Player 13.0.0.182 installed with Internet Explorer 11 will automatically be updated to the latest Internet Explorer 11 version, which will include Adobe Flash Player 13.0.0.206 for Windows 8.1.

These updates resolve a buffer overflow vulnerability that could result in arbitrary code execution (CVE-2014-0515).

| Affected Software | Recommended Player Update | Availability |
|---|---|---|
| Flash Player 13.0.0.182 and earlier versions for Windows | 13.0.0.206 | Flash Player Download Center |
| Flash Player 13.0.0.201 and earlier versions for Macintosh | 13.0.0.206 | Flash Player Download Center |
| Flash Player 13.0.0.182 and earlier versions for Windows (network distribution) | 13.0.0.206 | Flash Player Licensing |
| Flash Player 13.0.0.201 and earlier versions for Macintosh (network distribution) | 13.0.0.206 | Flash Player Licensing |
| Flash Player 11.2.202.350 and earlier for Linux | 11.2.202.356 | Flash Player Download Center |
| | 13.0.0.206 | Google Chrome Releases |

| | | |
|---|---|---|
| Flash Player 13.0.0.182 and earlier for Chrome (Windows, Macintosh and Linux) | | |
| Flash Player 13.0.0.182 and earlier in Internet Explorer 10 for Windows 8.0 | 13.0.0.206 | Microsoft Security Advisory |
| Flash Player 13.0.0.182 and earlier in Internet Explorer 11 for Windows 8.1 | 13.0.0.206 | Microsoft Security Advisory |

## Acknowledgments

Adobe would like to thank Alexander Polyakov of Kaspersky Labs for reporting CVE-2014-0515 and for working with Adobe to help protect our customers.

# Severity ratings

## Priority and Severity rating systems for Security Bulletins

The Adobe Priority Rating System is a guideline to help our customers in managed environments prioritize Adobe security updates. We base our priority rankings on historical attack patterns for the relevant product, the type of vulnerability, the platform(s) affected, and any potential mitigations that are in place.

The definitions of the priority ratings are:

| Rating | Definition |
|---|---|
| **Priority 1** | This update resolves vulnerabilities being targeted, or which have a higher risk of being targeted, by exploit(s) in the wild for a given product version and platform. Adobe recommends administrators install the update as soon as possible. (for example, within 72 hours). |
| **Priority 2** | This update resolves vulnerabilities in a product that has historically been at elevated risk. There are currently no known exploits. Based on previous experience, we do not anticipate exploits are imminent. As a best practice, Adobe recommends administrators install the update soon (for example, within 30 days). |
| **Priority 3** | This update resolves vulnerabilities in a product that has historically not been a target for attackers. Adobe recommends administrators install the update at their discretion. |

The Adobe Severity Rating System is a guideline to help our developers assess the security impact of known software vulnerabilities.

The definitions of the severity ratings are:

| Rating | Definition |
|---|---|
| **Critical** | A vulnerability, which, if exploited would allow malicious native-code to execute, potentially without a user being aware. |
| **Important** | A vulnerability, which, if exploited would compromise data security, potentially allowing access to confidential data, or could compromise processing resources in a user's computer. |
| **Moderate** | A vulnerability that is limited to a significant degree by factors such as default configuration, auditing, or is difficult to exploit. |

| | |
|---|---|
| **Low** | A vulnerability that has minimal impact and is extremely difficult to exploit. |

SECURITY BULLETINS
NOTIFICATION SERVICE
ALERT US
SEVERITY RATINGS
ACKNOWLEDGMENTS
PSIRT PGP Key

Choose your region **Products** **Downloads** **Learn & Support** **Company**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

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

**LODGED UNDER SEAL**

**FTC PROPOSED EXHIBIT __27__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

PCi Security Standards Council™

# Payment Card Industry (PCI)
# Data Security Standard

## Requirements and Security Assessment Procedures

**Version 2.0**

October 2010

# Document Changes

| Date | Version | Description | Pages |
|---|---|---|---|
| *October 2008* | *1.2* | *To introduce PCI DSS v1.2 as "PCI DSS Requirements and Security Assessment Procedures," eliminating redundancy between documents, and make both general and specific changes from* PCI DSS Security Audit Procedures v1.1. *For complete information, see* PCI Data Security Standard Summary of Changes from PCI DSS Version 1.1 to 1.2. | |
| *July 2009* | *1.2.1* | *Add sentence that was incorrectly deleted between PCI DSS v1.1 and v1.2.* | *5* |
| | | *Correct "then" to "than" in testing procedures 6.3.7.a and 6.3.7.b.* | *32* |
| | | *Remove grayed-out marking for "in place" and "not in place" columns in testing procedure 6.5.b.* | *33* |
| | | *For Compensating Controls Worksheet – Completed Example, correct wording at top of page to say "Use this worksheet to define compensating controls for any requirement noted as 'in place' via compensating controls."* | *64* |
| *October 2010* | *2.0* | *Update and implement changes from v1.2.1. For details, please see* "PCI DSS - Summary of Changes from PCI DSS Version 1.2.1 to 2.0." | |

# Table of Contents

# Introduction and PCI Data Security Standard Overview

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks. Below is a high-level overview of the 12 PCI DSS requirements.

## PCI Data Security Standard – High Level Overview

| | |
|---|---|
| **Build and Maintain a Secure Network** | **1.** Install and maintain a firewall configuration to protect cardholder data<br>**2.** Do not use vendor-supplied defaults for system passwords and other security parameters |
| **Protect Cardholder Data** | **3.** Protect stored cardholder data<br>**4.** Encrypt transmission of cardholder data across open, public networks |
| **Maintain a Vulnerability Management Program** | **5.** Use and regularly update anti-virus software or programs<br>**6.** Develop and maintain secure systems and applications |
| **Implement Strong Access Control Measures** | **7.** Restrict access to cardholder data by business need to know<br>**8.** Assign a unique ID to each person with computer access<br>**9.** Restrict physical access to cardholder data |
| **Regularly Monitor and Test Networks** | **10.** Track and monitor all access to network resources and cardholder data<br>**11.** Regularly test security systems and processes. |
| **Maintain an Information Security Policy** | **12.** Maintain a policy that addresses information security for all personnel. |

This document, *PCI Data Security Standard Requirements and Security Assessment Procedures*, combines the 12 PCI DSS requirements and corresponding testing procedures into a security assessment tool. It is designed for use during PCI DSS compliance assessments as part of an entity's validation process. The following sections provide detailed guidelines and best practices to assist entities prepare for, conduct, and report the results of a PCI DSS assessment. The PCI DSS Requirements and Testing Procedures begin on **page 19.**

The PCI Security Standards Council (PCI SSC) website (www.pcisecuritystandards.org) contains a number of additional resources, including:

- Attestations of Compliance
- *Navigating PCI DSS: Understanding the Intent of the Requirements*
- The *PCI DSS and PA-DSS Glossary of Terms, Abbreviations and Acronyms*
- Frequently Asked Questions (FAQs)
- Information Supplements and Guidelines

Please refer to www.pcisecuritystandards.org for more information.

***Note**: Information Supplements complement the PCI DSS and identify additional considerations and recommendations for meeting PCI DSS requirements – they do not change, eliminate or supersede the PCI DSS or any of its requirements.*

# PCI DSS Applicability Information

PCI DSS applies wherever account data is stored, processed or transmitted. *Account Data* consists of *Cardholder Data* plus *Sensitive Authentication Data*, as follows:

| ***Cardholder Data includes:*** | ***Sensitive Authentication Data includes:*** |
|---|---|
| ▪ Primary Account Number (PAN)<br>▪ Cardholder Name<br>▪ Expiration Date<br>▪ Service Code | ▪ Full magnetic stripe data or equivalent on a chip<br>▪ CAV2/CVC2/CVV2/CID<br>▪ PINs/PIN blocks |

***The primary account number is the defining factor in the applicability of PCI DSS requirements.*** PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed or transmitted, PCI DSS requirements do not apply.

If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with all PCI DSS requirements ***except*** Requirements 3.3 and 3.4, which apply only to PAN.

PCI DSS represents a minimum set of control objectives which may be enhanced by local, regional and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personally identifiable information or other data elements (for example, cardholder name), or define an entity's disclosure practices related to consumer information. Examples include legislation related to consumer data protection, privacy, identity theft, or data security. PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements.

The following table illustrates commonly used elements of cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited, and whether each data element must be protected. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

| | | Data Element | Storage Permitted | Render Stored Account Data Unreadable per Requirement 3.4 |
|---|---|---|---|---|
| Account Data | Cardholder Data | Primary Account Number (PAN) | Yes | Yes |
| | | Cardholder Name | Yes | No |
| | | Service Code | Yes | No |
| | | Expiration Date | Yes | No |
| | Sensitive Authentication Data[1] | Full Magnetic Stripe Data[2] | No | Cannot store per Requirement 3.2 |
| | | CAV2/CVC2/CVV2/CID | No | Cannot store per Requirement 3.2 |
| | | PIN/PIN Block | No | Cannot store per Requirement 3.2 |

PCI DSS requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.

PCI DSS ***only applies*** if PANs are stored, processed and/or transmitted.

[1] *Sensitive authentication data must not be stored after authorization (even if encrypted).*

[2] *Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.*

# Relationship between PCI DSS and PA-DSS

Use of a PA-DSS compliant application by itself does not make an entity PCI DSS compliant, since that application must be implemented into a PCI DSS compliant environment and according to the PA-DSS Implementation Guide provided by the payment application vendor (per PA-DSS Requirement 13.1).

The requirements for the Payment Application Data Security Standard (PA-DSS) are derived from the *PCI DSS Requirements and Security Assessment Procedures* (this document). The PA-DSS details what a payment application must support to facilitate a customer's PCI DSS compliance.

Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card verification codes and values (CAV2, CID, CVC2, CVV2), and PINs and PIN blocks, along with the damaging fraud resulting from these breaches.

Just a few of the ways payment applications can prevent compliance include:

- Storage of magnetic stripe data and/or equivalent data from the chip in the customer's network after authorization;
- Applications that require customers to disable other features required by the PCI DSS, like anti-virus software or firewalls, in order to get the payment application to work properly; and
- Vendors' use of unsecured methods to connect to the application to provide support to the customer.

The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.

Please note the following regarding PA-DSS applicability:

- PA-DSS ***does*** apply to payment applications that are typically sold and installed "off the shelf" without much customization by software vendors.
- PA-DSS ***does not*** apply to payment applications developed by merchants and service providers if used only in-house (not sold, distributed, or licensed to a third party), since this in-house developed payment application would be covered as part of the merchant's or service provider's normal PCI DSS compliance.

For detailed guidance on determining whether PA-DSS applies to a given payment application, please refer to the PA-DSS Requirements and Security Assessment Procedures, which can be found at www.pcisecuritystandards.org.

# Scope of Assessment for Compliance with PCI DSS Requirements

The PCI DSS security requirements apply to all system components. In the context of PCI DSS, "system components" are defined as any network component, server, or application that is included in or connected to the cardholder data environment. "System components" also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. The cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (for example, Internet) applications.

The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope. To confirm the accuracy and appropriateness of PCI DSS scope, perform the following:

- The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined cardholder data environment (CDE).
- Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).
- The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE unless such data is deleted or migrated/consolidated into the currently defined CDE.
- The entity retains documentation that shows how PCI DSS scope was confirmed and the results, for assessor review and/or for reference during the next annual PCI SCC scope confirmation activity.

### *Network Segmentation*

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that may reduce:

- The scope of the PCI DSS assessment
- The cost of the PCI DSS assessment
- The cost and difficulty of implementing and maintaining PCI DSS controls
- The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)

Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment. Network segmentation can be achieved through a number of physical or logical means, such as properly configured internal network firewalls, routers with strong access control lists, or other technologies that restrict access to a particular segment of a network.

An important prerequisite to reduce the scope of the cardholder data environment is a clear understanding of business needs and processes related to the storage, processing or transmission of cardholder data. Restricting cardholder data to as few locations as possible by elimination of unnecessary data, and consolidation of necessary data, may require reengineering of long-standing business practices.

Documenting cardholder data flows via a dataflow diagram helps fully understand all cardholder data flows and ensures that any network segmentation is effective at isolating the cardholder data environment.

If network segmentation is in place and being used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment. At a high level, adequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not. However, the adequacy of a specific implementation of network segmentation is highly variable and dependent upon a number of factors, such as a given network's configuration, the technologies deployed, and other controls that may be implemented.

*Appendix D: Segmentation and Sampling of Business Facilities/System Components* provides more information on the effect of network segmentation and sampling on the scope of a PCI DSS assessment.

### *Wireless*

If wireless technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, “line-busting”), or if a wireless local area network (WLAN) is connected to, or part of, the cardholder data environment (for example, not clearly separated by a firewall), the PCI DSS requirements and testing procedures for wireless environments apply and must be performed (for example, Requirements 1.2.3, 2.1.1, and 4.1.1). Before wireless technology is implemented, an entity should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.

### *Third Parties/Outsourcing*

For service providers required to undergo an annual onsite assessment, compliance validation must be performed on all system components in the cardholder data environment.

A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment.

For those entities that outsource storage, processing, or transmission of cardholder data to third-party service providers, the Report on Compliance (ROC) must document the role of each service provider, clearly identifying which requirements apply to the assessed entity and which apply to the service provider. There are two options for third-party service providers to validate compliance:

1) They can undergo a PCI DSS assessment on their own and provide evidence to their customers to demonstrate their compliance; or
2) If they do not undergo their own PCI DSS assessment, they will need to have their services reviewed during the course of each of their customers' PCI DSS assessments.

See the bullet beginning "For managed service provider (MSP) reviews," in Item 3, "Details about Reviewed Environment," in the "Instructions and Content for Report on Compliance" section, below, for more information.

Additionally, merchants and service providers must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data. *Refer to Requirement 12.8 in this document for details.*

### *Sampling of Business Facilities/System Components*

Sampling is not a PCI DSS requirement. However, after considering the overall scope and complexity of the environment being assessed, the assessor may independently select representative samples of business facilities/system components in order to assess PCI DSS requirements. These samples must be defined first for business facilities and then for system components within each selected business facility. Samples must be a representative selection of all of the types and locations of business facilities, as well as types of system components within selected business facilities. Samples must be sufficiently large to provide the assessor with assurance that controls are implemented as expected.

Sampling of business facilities/system components for an assessment does not reduce the scope of the cardholder data environment or the applicability of PCI DSS requirements. Whether or not sampling is to be used, PCI DSS requirements apply to the entire cardholder data environment. If sampling is used, each sample must be assessed against all applicable PCI DSS requirements. Sampling of the PCI DSS Requirements themselves is not permitted.

Examples of business facilities include but are not limited to: corporate offices, stores, franchise locations, processing facilities, data centers, and other facility types in different locations. Sampling should include system components within each selected business facility. For example, for each business facility selected, include a variety of operating systems, functions, and applications that are applicable to the area under review.

As an example, the assessor may define a sample at a business facility to include Sun servers running Apache WWW, Windows servers running Oracle, mainframe systems running legacy card processing applications, data transfer servers running HP-UX, and Linux Servers running MYSQL. If all applications run from a single version of an OS (for example, Windows 7 or Solaris 10), then the sample should still include a variety of applications (for example, database servers, web servers, data transfer servers).

When independently selecting samples of business facilities/system components, assessors should consider the following:

- If there are standard, centralized PCI DSS security and operational processes and controls in place that ensure consistency and that each business facility/system component must follow, the sample can be smaller than if there are no standard processes/controls in place. The sample must be large enough to provide the assessor with reasonable assurance that all business facilities/system components are configured per the standard processes.
- If there is more than one type of standard security and/or operational process in place (for example, for different types of business facilities/system components), the sample must be large enough to include business facilities/system components secured with each type of process.

- If there are no standard PCI DSS processes/controls in place and each business facility/system component is managed through non-standard processes, the sample must be larger for the assessor to be assured that each business facility/system component has implemented PCI DSS requirements appropriately.

For each instance where sampling is used, the assessor must:

- Document the rationale behind the sampling technique and sample size,
- Document and validate the standardized PCI DSS processes and controls used to determine sample size, and
- Explain how the sample is appropriate and representative of the overall population.

Assessors must revalidate the sampling rationale for each assessment. If sampling is to be used, different samples of business facilities and system components must be selected for each assessment.

***Please also refer to:***
Appendix D: Segmentation and Sampling of Business Facilities/System Components.

### *Compensating Controls*

On an annual basis, any compensating controls must be documented, reviewed and validated by the assessor and included with the Report on Compliance submission, per *Appendix B: Compensating Controls* and *Appendix C: Compensating Controls Worksheet.*

For each and every compensating control, the Compensating Controls Worksheet *(Appendix C)* **must** be completed. Additionally, compensating control results should be documented in the ROC in the corresponding PCI DSS requirement section.

See the above-mentioned *Appendices B* and *C* for more details on "compensating controls."

# Instructions and Content for Report on Compliance

This document must be used as the template for creating the *Report on Compliance*. The assessed entity should follow each payment brand's respective reporting requirements to ensure each payment brand acknowledges the entity's compliance status. Contact each payment brand to determine reporting requirements and instructions.

### *Report Content and Format*

Follow these instructions for report content and format when completing a Report on Compliance:

1. **Executive Summary**

   Include the following:

   - Describe the entity's payment card business, including:
     - Their business role with payment cards, which is how and why they store, process, and/or transmit cardholder data

       ***Note:*** *This is not intended to be a cut-and-paste from the entity's web site, but should be a tailored description that shows the assessor understands payment and the entity's role.*
     - How they process payment (directly, indirectly, etc.)
     - What types of payment channels they serve, such as card-not-present (for example, mail-order-telephone-order (MOTO), e-Commerce), or card-present
     - Any entities that they connect to for payment transmission or processing, including processor relationships
   - A high-level network diagram (either obtained from the entity or created by assessor) of the entity's networking topography that includes:
     - Connections into and out of the network
     - Critical components within the cardholder data environment, including POS devices, systems, databases, and web servers, as applicable
     - Other necessary payment components, as applicable

## 2. Description of Scope of Work and Approach Taken

Describe the scope, per the Scope of Assessment section of this document, including the following:

- Document how the assessor validated the accuracy of the PCI DSS scope for the assessment, including:
  - The methods or processes used to identify and document all existences of cardholder data
  - How the results were evaluated and documented
  - How the effectiveness and accuracy of the methods used were verified
  - That the assessor validates that the scope of the assessment is accurate and appropriate.
- Environment on which assessment focused (for example, client's Internet access points, internal corporate network, processing connections)
- If network segmentation is in place and was used to reduce scope of the PCI DSS review, briefly explain that segmentation and how assessor validated the effectiveness of the segmentation
- If sampling is used during the assessment, for each sample set selected (of business facilities/system components) document the following:
  - Total population
  - Number sampled
  - Rationale for sample selected
  - Description of the standardized PCI DSS security and operational processes and controls used to determine sample size, and how the processes/controls were validated
  - How the sample is appropriate and representative of the overall population
  - Description of any locations or environments that store, process, or transmit cardholder data that were EXCLUDED from the scope of the review, and why these locations/environments were excluded
- List any wholly-owned entities that require compliance with the PCI DSS, and whether they are reviewed separately or as part of this assessment
- List any international entities that require compliance with the PCI DSS, and whether they are reviewed separately or as part of this assessment
- List any wireless LANs and/or wireless payment applications (for example, POS terminals) that are connected to, or could impact the security of the cardholder data environment, and describe security in place for these wireless environments
- The version of the PCI DSS Requirements and Security Assessment Procedures document used to conduct the assessment

### 3. Details about Reviewed Environment

Include the following details in this section:

- A diagram of each piece of the communication link, including LAN, WAN or Internet
- Description of cardholder data environment, for example:
  - Document transmission and processing of cardholder data, including authorization, capture, settlement, chargeback and other flows as applicable
  - List of files and tables that store cardholder data, supported by an inventory created (or obtained from the client) and retained by the assessor in the work papers. This inventory should include, for each cardholder data store (file, table, etc.):
    - List all of the elements of stored cardholder data
    - How data is secured
    - How access to data stores are logged
- List of hardware and critical software in use in the cardholder data environment, along with description of function/use for each
- List of service providers and other third parties with which the entity shares cardholder data

  ***Note:*** *These entities are subject to PCI DSS Requirement 12.8.*)
- List of third-party payment application products and versions numbers in use, including whether each payment application has been validated according to PA-DSS. Even if a payment application has been PA-DSS validated, the assessor still needs to verify that the application has been implemented in a PCI DSS compliant manner and environment, and according to the payment application vendor's *PA-DSS Implementation Guide.*

  ***Note:*** *It is not a PCI DSS requirement to use PA-DSS validated applications. Please consult with each payment brand individually to understand their PA-DSS compliance requirements.)*
- List of individuals interviewed, their organizations, titles, and topics covered
- List of documentation reviewed
- For managed service provider (MSP) reviews, the assessor must clearly identify which requirements in this document apply to the MSP (and are included in the review), and which are not included in the review and are the responsibility of the MSP's customers to include in their reviews. Include information about which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans, and which IP addresses are the responsibility of the MSP's customers to include in their own quarterly scans.

4. **Contact Information and Report Date**

Include:

- Contact information for merchant or service provider and assessor
- Timeframe of assessment—specify the duration and the time period over which the assessment occurred
- Date of report

5. **Quarterly Scan Results**

- Summarize the four most recent quarterly ASV scan results in the Executive Summary as well as in comments at Requirement 11.2.2.

> ***Note:*** *It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies:*
>
> *1) The most recent scan result was a passing scan,*
>
> *2) The entity has documented policies and procedures requiring quarterly scanning going forward, and*
>
> *3) Any vulnerabilities noted in the initial scan have been corrected as shown in a re-scan.*
>
> *For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.*

- Scan must cover all externally accessible (Internet-facing) IP addresses in existence at the entity, in accordance with the *PCI Approved Scanning Vendors (ASV) Program Guide.*

6. **Findings and Observations**

Summarize in the Executive Summary any findings that may not fit into the standard Report on Compliance template format.

All assessors *must:*

- Use the Detailed PCI DSS Requirements and Security Assessment Procedures template to provide detailed report descriptions and findings on each requirement and sub-requirement.
- Ensure that all N/A responses are clearly explained.
- Review and document any compensating controls considered to conclude that a control is in place.

*See* "Compensating Controls" section above and *Appendices B* and *C* for more details on compensating controls.

### *Revalidation of Open Items*

A "controls in place" report is required to verify compliance. The report is considered non-compliant if it contains "open items," or items that will be finished at a future date. The merchant/service provider must address these items before validation is completed. After open items are addressed by the merchant/service provider, the assessor will then reassess to validate that the remediation occurred and that all requirements are satisfied. After revalidation, the assessor will issue a new Report on Compliance, verifying that the cardholder data environment is fully compliant, and submit it consistent with instructions (see below).

### *PCI DSS Compliance – Completion Steps*

1. Complete the Report on Compliance (ROC) according to the section above entitled “Instructions and Content for Report on Compliance.”
2. Ensure passing vulnerability scan(s) have been completed by a PCI SSC Approved Scanning Vendor (ASV), and obtain evidence of passing scan(s) from the ASV.
3. Complete the Attestation of Compliance for Service Providers or Merchants, as applicable, in its entirety. Attestations of Compliance are available on the PCI SSC website (www.pcisecuritystandards.org).
4. Submit the ROC, evidence of a passing scan, and the Attestation of Compliance, along with any other requested documentation, to the acquirer (for merchants) or to the payment brand or other requester (for service providers).

# Detailed PCI DSS Requirements and Security Assessment Procedures

For the *PCI DSS Requirements and Security Assessment Procedures,* the following defines the table column headings:

- **PCI DSS Requirements** – This column defines the Data Security Standard and lists requirements to achieve PCI DSS compliance; compliance will be validated against these requirements.
- **Testing Procedures** – This column shows processes to be followed by the assessor to validate that PCI DSS requirements are "in place."
- **In Place** – This column must be used by the assessor to provide a brief description of the controls which were validated as "in place" for each requirement, including descriptions of controls found to be in place as a result of compensating controls, or as a result of a requirement being "Not Applicable."

> ***Note:*** *This column must not be used for controls that are not yet in place or for open items to be completed at a future date.*

- **Not in Place** – This column must be used by the assessor to provide a brief description of controls that are not in place. Note that a non-compliant report should not be submitted to a payment brand or acquirer unless specifically requested. , For further instructions on non-compliant reports, please refer to the Attestations of Compliance, available on the PCI SSC website (www.pcisecuritystandards.org).
- **Target Date/Comments** – For those controls "Not in Place" the assessor may include a target date that the merchant or service provider expects to have controls "In Place." Any additional notes or comments may be included here as well.

## Build and Maintain a Secure Network

### *Requirement 1: Install and maintain a firewall configuration to protect cardholder data*

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **1.1** Establish firewall and router configuration standards that include the following: | **1.1** Obtain and inspect the firewall and router configuration standards and other documentation specified below to verify that standards are complete. Complete the following: | | | |
| **1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configurations | **1.1.1** Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations. | | | |
| **1.1.2** Current network diagram with all connections to cardholder data, including any wireless networks | **1.1.2.a** Verify that a current network diagram (for example, one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks. | | | |
| | **1.1.2.b** Verify that the diagram is kept current. | | | |
| **1.1.3** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone | **1.1.3.a** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. | | | |
| | **1.1.3.b** Verify that the current network diagram is consistent with the firewall configuration standards. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **1.1.4** Description of groups, roles, and responsibilities for logical management of network components | **1.1.4** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components. | | | |
| **1.1.5** Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.<br>Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP. | **1.1.5.a** Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols. | | | |
| | **1.1.5.b** Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. | | | |
| **1.1.6** Requirement to review firewall and router rule sets at least every six months | **1.1.6.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months. | | | |
| | **1.1.6.b** Obtain and examine documentation to verify that the rule sets are reviewed at least every six months. | | | |
| **1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.<br>***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.* | **1.2** Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows: | | | |
| **1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. | **1.2.1.a** Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented. | | | |
| | **1.2.1.b** Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments. |
|---|---|---|---|---|
| **1.2.2** Secure and synchronize router configuration files. | **1.2.2** Verify that router configuration files are secure and synchronized—for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations. | | | |
| **1.2.3** Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. | **1.2.3** Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. | | | |
| **1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment. | **1.3** Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—to determine that there is no direct access between the Internet and system components in the internal cardholder network segment, as detailed below. | | | |
| **1.3.1** Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. | **1.3.1** Verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. | | | |
| **1.3.2** Limit inbound Internet traffic to IP addresses within the DMZ. | **1.3.2** Verify that inbound Internet traffic is limited to IP addresses within the DMZ. | | | |
| **1.3.3** Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment. | **1.3.3** Verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment. | | | |
| **1.3.4** Do not allow internal addresses to pass from the Internet into the DMZ. | **1.3.4** Verify that internal addresses cannot pass from the Internet into the DMZ. | | | |
| **1.3.5** Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. | **1.3.5** Verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **1.3.6** Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.) | **1.3.6** Verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.) | | | |
| **1.3.7** Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | **1.3.7** Verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks. | | | |
| **1.3.8** Do not disclose private IP addresses and routing information to unauthorized parties.<br>***Note:*** *Methods to obscure IP addressing may include, but are not limited to:*<br>▪ *Network Address Translation (NAT)*<br>▪ *Placing servers containing cardholder data behind proxy servers/firewalls or content caches,*<br>▪ *Removal or filtering of route advertisements for private networks that employ registered addressing,*<br>▪ *Internal use of RFC1918 address space instead of registered addresses.* | **1.3.8.a** Verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. | | | |
| | **1.3.8.b** Verify that any disclosure of private IP addresses and routing information to external entities is authorized. | | | |
| **1.4** Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network. | **1.4.a** Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active. | | | |
| | **1.4.b** Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by users of mobile and/or employee-owned computers. | | | |

## Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **2.1** Always change vendor-supplied defaults **before** installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts. | **2.1** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.) | | | |
| **2.1.1** For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. | **2.1.1** Verify the following regarding vendor default settings for wireless environments: | | | |
| | **2.1.1.a** Verify encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions | | | |
| | **2.1.1.b** Verify default SNMP community strings on wireless devices were changed. | | | |
| | **2.1.1.c** Verify default passwords/passphrases on access points were changed. | | | |
| | **2.1.1.d** Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks. | | | |
| | **2.1.1.e** Verify other security-related wireless vendor defaults were changed, if applicable. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.<br>Sources of industry-accepted system hardening standards may include, but are not limited to:<br>▪ Center for Internet Security (CIS)<br>▪ International Organization for Standardization (ISO)<br>▪ SysAdmin Audit Network Security (SANS) Institute<br>▪ National Institute of Standards Technology (NIST) | **2.2.a** Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards. | | | |
| | **2.2.b** Verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.2. | | | |
| | **2.2.c** Verify that system configuration standards are applied when new systems are configured. | | | |
| | **2.2.d** Verify that system configuration standards include each item below (2.2.1 – 2.2.4). | | | |
| **2.2.1** Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)<br>***Note:*** *Where virtualization technologies are in use, implement only one primary function per virtual system component.* | **2.2.1.a** For a sample of system components, verify that only one primary function is implemented per server. | | | |
| | **2.2.1.b** If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **2.2.2** Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system.<br>Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. | **2.2.2.a** For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that only necessary services or protocols are enabled. | | | |
| | **2.2.2.b** Identify any enabled insecure services, daemons, or protocols. Verify they are justified and that security features are documented and implemented. | | | |
| **2.2.3** Configure system security parameters to prevent misuse. | **2.2.3.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components. | | | |
| | **2.2.3.b** Verify that common security parameter settings are included in the system configuration standards.. | | | |
| | **2.2.3.c** For a sample of system components, verify that common security parameters are set appropriately. | | | |
| **2.2.4** Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. | **2.2.4.a** For a sample of system components, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. | | | |
| | **2.2.4.b**. Verify enabled functions are documented and support secure configuration. | | | |
| | **2.2.4.c**. Verify that only documented functionality is present on the sampled system components. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **2.3** Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. | **2.3** For a sample of system components, verify that non-console administrative access is encrypted by performing the following: | | | |
| | **2.3.a** Observe an administrator log on to each system to verify that a strong encryption method is invoked before the administrator's password is requested. | | | |
| | **2.3.b** Review services and parameter files on systems to determine that Telnet and other remote login commands are not available for use internally. | | | |
| | **2.3.c** Verify that administrator access to the web-based management interfaces is encrypted with strong cryptography. | | | |
| **2.4** Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.* | **2.4** Perform testing procedures **A.1.1** through **A.1.4** detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data. | | | |

# Protect Cardholder Data

## *Requirement 3: Protect stored cardholder data*

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography" and other PCI DSS terms.

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **3.1** Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows. | **3.1** Obtain and examine the policies, procedures and processes for data retention and disposal, and perform the following: | | | |
| **3.1.1** Implement a data retention and disposal policy that includes:<br>▪ Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements<br>▪ Processes for secure deletion of data when no longer needed<br>▪ Specific retention requirements for cardholder data<br>▪ A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements | **3.1.1.a** Verify that policies and procedures are implemented and include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons). | | | |
| | **3.1.1.b** Verify that policies and procedures include provisions for secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data. | | | |
| | **3.1.1.c** Verify that policies and procedures include coverage for all storage of cardholder data. | | | |
| | **3.1.1.d** Verify that policies and procedures include at least one of the following:<br>A programmatic process (automatic or manual) to remove, at least quarterly, stored cardholder data that exceeds requirements defined in the data retention policy<br>Requirements for a review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements defined in the data retention policy. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| | **3.1.1.e** For a sample of system components that store cardholder data, verify that the data stored does not exceed the requirements defined in the data retention policy. | | | |
| **3.2** Do not store sensitive authentication data after authorization (even if encrypted).<br>Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:<br>***Note:*** *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.* | **3.2.a** For issuers and/or companies that support issuing services and store sensitive authentication data, verify there is a business justification for the storage of sensitive authentication data, and that the data is secured. | | | |
| | **3.2.b** For all other entities, if sensitive authentication data is received and deleted, obtain and review the processes for securely deleting the data to verify that the data is unrecoverable. | | | |
| | **3.2.c** For each item of sensitive authentication data below, perform the following steps: | | | |
| **3.2.1** Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.<br>***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:*<br>▪ *The cardholder's name*<br>▪ *Primary account number (PAN)*<br>▪ *Expiration date*<br>▪ *Service code*<br>*To minimize risk, store only these data elements as needed for business.* | **3.2.1** For a sample of system components, examine data sources, including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored under any circumstance:<br>▪ Incoming transaction data<br>▪ All logs (for example, transaction, history, debugging, error)<br>▪ History files<br>▪ Trace files<br>▪ Several database schemas<br>▪ Database contents | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **3.2.2** Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. | **3.2.2** For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance:<br>▪ Incoming transaction data<br>▪ All logs (for example, transaction, history, debugging, error)<br>▪ History files<br>▪ Trace files<br>▪ Several database schemas<br>▪ Database contents | | | |
| **3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block. | **3.2.3** For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance:<br>▪ Incoming transaction data<br>▪ All logs (for example, transaction, history, debugging, error)<br>▪ History files<br>▪ Trace files<br>▪ Several database schemas<br>▪ Database contents | | | |
| **3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).<br>***Notes:***<br>▪ *This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.*<br>▪ *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts.* | **3.3** Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **3.4** Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:<br>▪ One-way hashes based on strong cryptography (hash must be of the entire PAN)<br>▪ Truncation (hashing cannot be used to replace the truncated segment of PAN)<br>▪ Index tokens and pads (pads must be securely stored)<br>▪ Strong cryptography with associated key-management processes and procedures<br>***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.* | **3.4.a** Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using any of the following methods:<br>▪ One-way hashes based on strong cryptography<br>▪ Truncation<br>▪ Index tokens and pads, with the pads being securely stored<br>▪ Strong cryptography, with associated key-management processes and procedures | | | |
| | **3.4.b** Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text). | | | |
| | **3.4.c** Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable. | | | |
| | **3.4.d** Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs. | | | |
| **3.4.1** If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts. | **3.4.1.a** If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local user account databases). | | | |
| | **3.4.1.b** Verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls). | | | |
| | **3.4.1.c** Verify that cardholder data on removable media is encrypted wherever stored.<br>***Note:*** *If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.* | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **3.5** Protect any keys used to secure cardholder data against disclosure and misuse:<br>***Note:*** *This requirement also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.* | **3.5** Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following: | | | |
| **3.5.1** Restrict access to cryptographic keys to the fewest number of custodians necessary. | **3.5.1** Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary. | | | |
| **3.5.2** Store cryptographic keys securely in the fewest possible locations and forms. | **3.5.2.a** Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys. | | | |
| | **3.5.2.b** Identify key storage locations to verify that keys are stored in the fewest possible locations and forms. | | | |
| **3.6** Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:<br>***Note:*** *Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.* | **3.6.a** Verify the existence of key-management procedures for keys used for encryption of cardholder data. | | | |
| | **3.6.b** For service providers only: If the service provider shares keys with their customers for transmission or storage of cardholder data, verify that the service provider provides documentation to customers that includes guidance on how to securely transmit, store and update customer's keys, in accordance with Requirements 3.6.1 through 3.6.8 below. | | | |
| | **3.6.c** Examine the key-management procedures and perform the following: | | | |
| **3.6.1** Generation of strong cryptographic keys | **3.6.1** Verify that key-management procedures are implemented to require the generation of strong keys. | | | |
| **3.6.2** Secure cryptographic key distribution | **3.6.2** Verify that key-management procedures are implemented to require secure key distribution. | | | |
| **3.6.3** Secure cryptographic key storage | **3.6.3** Verify that key-management procedures are implemented to require secure key storage. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **3.6.4** Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). | **3.6.4** Verify that key-management procedures are implemented to require periodic key changes at the end of the defined cryptoperiod. | | | |
| **3.6.5** Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised.<br>***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.* | **3.6.5.a** Verify that key-management procedures are implemented to require the retirement of keys when the integrity of the key has been weakened. | | | |
| | **3.6.5.b** Verify that the key-management procedures are implemented to require the replacement of known or suspected compromised keys. | | | |
| | **3.6.5.c** If retired or replaced cryptographic keys are retained, verify that these keys are not used for encryption operations. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **3.6.6** If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key).<br>***Note:*** *Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.* | **3.6.6** Verify that manual clear-text key-management procedures require split knowledge and dual control of keys. | | | |
| **3.6.7** Prevention of unauthorized substitution of cryptographic keys. | **3.6.7** Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys. | | | |
| **3.6.8** Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities. | **3.6.8** Verify that key-management procedures are implemented to require key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities. | | | |

## Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments..

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **4.1** Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.<br>*Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:*<br>▪ The Internet<br>▪ Wireless technologies,<br>▪ Global System for Mobile communications (GSM)<br>▪ General Packet Radio Service (GPRS). | **4.1** Verify the use of security protocols wherever cardholder data is transmitted or received over open, public networks.<br>Verify that strong cryptography is used during data transmission, as follows: | | | |
| | **4.1.a** Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit. | | | |
| | **4.1.b** Verify that only trusted keys and/or certificates are accepted. | | | |
| | **4.1.c** Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations. | | | |
| | **4.1.d** Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.) | | | |
| | **4.1.e** For SSL/TLS implementations:<br>▪ Verify that HTTPS appears as a part of the browser Universal Record Locator (URL).<br>▪ Verify that no cardholder data is required when HTTPS does not appear in the URL. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **4.1.1** Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.<br>***Note:*** *The use of WEP as a security control was prohibited as of 30 June 2010.* | **4.1.1** For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission. | | | |
| **4.2** Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.). | **4.2.a** Verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. | | | |
| | **4.2.b** Verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies. | | | |

## Maintain a Vulnerability Management Program

### *Requirement 5: Use and regularly update anti-virus software or programs*

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **5.1** Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). | **5.1** For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists. | | | |
| **5.1.1** Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. | **5.1.1** For a sample of system components, verify that all anti-virus programs detect, remove, and protect against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits). | | | |
| **5.2** Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs. | **5.2** Verify that all anti-virus software is current, actively running, and generating logs by performing the following: | | | |
| | **5.2.a** Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions. | | | |
| | **5.2.b** Verify that the master installation of the software is enabled for automatic updates and periodic scans. | | | |
| | **5.2.c** For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled. | | | |
| | **5.2.d** For a sample of system components, verify that anti-virus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7. | | | |

## Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

***Note:** Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.*

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **6.1** Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.<br>***Note:** An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.* | **6.1.a** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed. | | | |
| | **6.1.b** Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **6.2** Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.<br>***Notes:***<br>▪ *Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component.*<br>▪ *The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.* | **6.2.a** Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities, and that a risk ranking is assigned to such vulnerabilities. (At minimum, the most critical, highest risk vulnerabilities should be ranked as "High." | | | |
| | **6.2.b** Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information. | | | |
| **6.3** Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following: | **6.3.a** Obtain and examine written software development processes to verify that the processes are based on industry standards and/or best practices. | | | |
| | **6.3.b** Examine written software development processes to verify that information security is included throughout the life cycle. | | | |
| | **6.3.c** Examine written software development processes to verify that software applications are developed in accordance with PCI DSS. | | | |
| | **6.3.d** From an examination of written software development processes, and interviews of software developers, verify that: | | | |
| **6.3.1** Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers. | **6.3.1** Custom application accounts, user IDs and/or passwords are removed before system goes into production or is released to customers. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **6.3.2** Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.<br>***Note:*** *This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.*<br>*Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.* | **6.3.2.a** Obtain and review policies to confirm that all custom application code changes must be reviewed (using either manual or automated processes) as follows:<br>▪ Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices.<br>▪ Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5).<br>▪ Appropriate corrections are implemented prior to release.<br>▪ Code review results are reviewed and approved by management prior to release. | | | |
| | **6.3.2.b** Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above. | | | |
| **6.4** Follow change control processes and procedures for all changes to system components. The processes must include the following: | **6.4** From an examination of change control processes, interviews with system and network administrators, and examination of relevant data (network configuration documentation, production and test data, etc.), verify the following: | | | |
| **6.4.1** Separate development/test and production environments | **6.4.1** The development/test environments are separate from the production environment, with access control in place to enforce the separation. | | | |
| **6.4.2** Separation of duties between development/test and production environments | **6.4.2** There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. | | | |
| **6.4.3** Production data (live PANs) are not used for testing or development | **6.4.3** Production data (live PANs) are not used for testing or development. | | | |
| **6.4.4** Removal of test data and accounts before production systems become active | **6.4.4** Test data and accounts are removed before a production system becomes active. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **6.4.5** Change control procedures for the implementation of security patches and software modifications. Procedures must include the following: | **6.4.5.a** Verify that change-control procedures related to implementing security patches and software modifications are documented and require items 6.4.5.1 – 6.4.5.4 below. | | | |
| | **6.4.5.b** For a sample of system components and recent changes/security patches, trace those changes back to related change control documentation. For each change examined, perform the following: | | | |
| **6.4.5.1** Documentation of impact. | **6.4.5.1** Verify that documentation of impact is included in the change control documentation for each sampled change. | | | |
| **6.4.5.2** Documented change approval by authorized parties. | **6.4.5.2** Verify that documented approval by authorized parties is present for each sampled change. | | | |
| **6.4.5.3** Functionality testing to verify that the change does not adversely impact the security of the system. | **6.4.5.3.a** For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system. | | | |
| | **6.4.5.3.b** For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production. | | | |
| **6.4.5.4** Back-out procedures. | **6.4.5.4** Verify that back-out procedures are prepared for each sampled change. | | | |
| **6.5** Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following:<br>***Note:*** *The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.* | **6.5.a** Obtain and review software development processes. Verify that processes require training in secure coding techniques for developers, based on industry best practices and guidance. | | | |
| | **6.5.b** Interview a sample of developers and obtain evidence that they are knowledgeable in secure coding techniques. | | | |
| | **6.5.c.** Verify that processes are in place to ensure that applications are not vulnerable to, at a minimum, the following: | | | |

FTC-0002134

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **6.5.1** Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. | **6.5.1** Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.) | | | |
| **6.5.2** Buffer overflow | **6.5.2** Buffer overflow (Validate buffer boundaries and truncate input strings.) | | | |
| **6.5.3** Insecure cryptographic storage | **6.5.3** Insecure cryptographic storage (Prevent cryptographic flaws) | | | |
| **6.5.4** Insecure communications | **6.5.4** Insecure communications (Properly encrypt all authenticated and sensitive communications) | | | |
| **6.5.5** Improper error handling | **6.5.5** Improper error handling (Do not leak information via error messages) | | | |
| **6.5.6** All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2).<br>***Note:*** *This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.* | **6.5.6** All "High" vulnerabilities as identified in PCI DSS Requirement 6.2. | | | |
| ***Note:*** *Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external):* | | | | |
| **6.5.7** Cross-site scripting (XSS) | **6.5.7** Cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.) | | | |
| **6.5.8** Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal) | **6.5.8** Improper Access Control, such as insecure direct object references, failure to restrict URL access, and directory traversal (Properly authenticate users and sanitize input. Do not expose internal object references to users.) | | | |
| **6.5.9** Cross-site request forgery (CSRF) | **6.5.9** Cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically submitted by browsers.) | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **6.6** For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by *either* of the following methods:<br>▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes<br>▪ Installing a web-application firewall in front of public-facing web applications | **6.6** For *public-facing* web applications, ensure that *either* one of the following methods are in place as follows:<br>▪ Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows:<br>– At least annually<br>– After any changes<br>– By an organization that specializes in application security<br>– That all vulnerabilities are corrected<br>– That the application is re-evaluated after the corrections<br>▪ Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks.<br>***Note:*** *"An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.* | | | |

## Implement Strong Access Control Measures

### *Requirement 7: Restrict access to cardholder data by business need to know*

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **7.1** Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following: | **7.1** Obtain and examine written policy for data control, and verify that the policy incorporates the following: | | | |
| **7.1.1** Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities. | **7.1.1** Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities. | | | |
| **7.1.2** Assignment of privileges is based on individual personnel's job classification and function | **7.1.2** Confirm that privileges are assigned to individuals based on job classification and function (also called "role-based access control" or RBAC). | | | |
| **7.1.3** Requirement for a documented approval by authorized parties specifying required privileges. | **7.1.3** Confirm that documented approval by authorized parties is required (in writing or electronically) for all access, and that it must specify required privileges. | | | |
| **7.1.4** Implementation of an automated access control system | **7.1.4** Confirm that access controls are implemented via an automated access control system. | | | |
| **7.2** Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.<br>This access control system must include the following: | **7.2** Examine system settings and vendor documentation to verify that an access control system is implemented as follows: | | | |
| **7.2.1** Coverage of all system components | **7.2.1** Confirm that access control systems are in place on all system components. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **7.2.2** Assignment of privileges to individuals based on job classification and function | **7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. | | | |
| **7.2.3** Default "deny-all" setting<br>***Note:*** *Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.* | **7.2.3** Confirm that the access control systems have a default "deny-all" setting. | | | |

## Requirement 8: Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions.. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

***Note:** These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. However, Requirements 8.1, 8.2 and 8.5.8 through 8.5.15 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).*

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **8.1** Assign all users a unique ID before allowing them to access system components or cardholder data. | **8.1** Verify that all users are assigned a unique ID for access to system components or cardholder data. | | | |
| **8.2** In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:<br>▪ Something you know, such as a password or passphrase<br>▪ Something you have, such as a token device or smart card<br>▪ Something you are, such as a biometric | **8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following:<br>▪ Obtain and examine documentation describing the authentication method(s) used.<br>▪ For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s). | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **8.3** Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.)<br>***Note:*** *Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.* | **8.3** To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that two of the three authentication methods are used. | | | |
| **8.4** Render all passwords unreadable during transmission and storage on all system components using strong cryptography. | **8.4.a** For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage. | | | |
| | **8.4.b** For service providers only, observe password files to verify that customer passwords are encrypted. | | | |
| **8.5** Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows: | **8.5** Review procedures and interview personnel to verify that procedures are implemented for user identification and authentication management, by performing the following: | | | |
| **8.5.1** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. | **8.5.1** Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to policy by performing the following:<br>▪ Obtain and examine an authorization form for each ID.<br>▪ Verify that the sampled user IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained), by tracing information from the authorization form to the system. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **8.5.2** Verify user identity before performing password resets. | **8.5.2** Examine password/authentication procedures and observe security personnel to verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the password is reset. | | | |
| **8.5.3** Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use. | **8.5.3** Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use. | | | |
| **8.5.4** Immediately revoke access for any terminated users. | **8.5.4** Select a sample of users terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed. | | | |
| **8.5.5** Remove/disable inactive user accounts at least every 90 days. | **8.5.5** Verify that inactive accounts over 90 days old are either removed or disabled. | | | |
| **8.5.6** Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use. | **8.5.6.a** Verify that any accounts used by vendors to access, support and maintain system components are disabled, and enabled only when needed by the vendor. | | | |
| | **8.5.6.b** Verify that vendor remote access accounts are monitored while being used. | | | |
| **8.5.7** Communicate authentication procedures and policies to all users who have access to cardholder data. | **8.5.7** Interview the users from a sample of user IDs, to verify that they are familiar with authentication procedures and policies. | | | |
| **8.5.8** Do not use group, shared, or generic accounts and passwords, or other authentication methods. | **8.5.8.a** For a sample of system components, examine user ID lists to verify the following:<br>▪ Generic user IDs and accounts are disabled or removed<br>▪ Shared user IDs for system administration activities and other critical functions do not exist<br>▪ Shared and generic user IDs are not used to administer any system components | | | |
| | **8.5.8.b** Examine authentication policies/procedures to verify that group and shared passwords or other authentication methods are explicitly prohibited. | | | |
| | **8.5.8.c** Interview system administrators to verify that group and shared passwords or other authentication methods are not distributed, even if requested. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **8.5.9** Change user passwords at least every 90 days. | **8.5.9.a** For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days. | | | |
| | **8.5.9.b** For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to change periodically and that non-consumer users are given guidance as to when, and under what circumstances, passwords must change. | | | |
| **8.5.10** Require a minimum password length of at least seven characters. | **8.5.10.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long. | | | |
| | **8.5.10.b** For service providers only, review internal processes and customer/user documentation to verify that that non-consumer user passwords are required to meet minimum length requirements. | | | |
| **8.5.11** Use passwords containing both numeric and alphabetic characters. | **8.5.11.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters. | | | |
| | **8.5.11.b** For service providers only, review internal processes and customer/user documentation to verify that non-consumer user passwords are required to contain both numeric and alphabetic characters. | | | |
| **8.5.12** Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used. | **8.5.12.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords. | | | |
| | **8.5.12.b** For service providers only, review internal processes and customer/user documentation to verify that new non-consumer user passwords cannot be the same as the previous four passwords. | | | |
| **8.5.13** Limit repeated access attempts by locking out the user ID after not more than six attempts. | **8.5.13.a** For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than six invalid logon attempts. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
|  | **8.5.13.b** For service providers only, review internal processes and customer/user documentation to verify that non-consumer user accounts are temporarily locked-out after not more than six invalid access attempts. |  |  |  |
| **8.5.14** Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID. | **8.5.14** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account. |  |  |  |
| **8.5.15** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. | **8.5.15** For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less. |  |  |  |
| **8.5.16** Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.<br>Restrict user direct access or queries to databases to database administrators. | **8.5.16.a** Review database and application configuration settings and verify that all users are authenticated prior to access. |  |  |  |
|  | **8.5.16.b** Verify that database and application configuration settings ensure that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures). |  |  |  |
|  | **8.5.16.c** Verify that database and application configuration settings restrict user direct access or queries to databases to database administrators. |  |  |  |
|  | **8.5.16.d** Review database applications and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes). |  |  |  |

## Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **9.1** Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. | **9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment.<br>▪ Verify that access is controlled with badge readers or other devices including authorized badges and lock and key.<br>▪ Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use. | | | |
| **9.1.1** Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.<br>***Note:*** *"Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.* | **9.1.1.a** Verify that video cameras and/or access control mechanisms are in place to monitor the entry/exit points to sensitive areas. | | | |
| | **9.1.1.b** Verify that video cameras and/or access control mechanisms are protected from tampering or disabling. | | | |
| | **9.1.1.c** Verify that video cameras and/or access control mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months. | | | |
| **9.1.2** Restrict physical access to publicly accessible network jacks.<br>For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized. | **9.1.2** Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized onsite personnel. Alternatively, verify that visitors are escorted at all times in areas with active network jacks. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **9.1.3** Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. | **9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted. | | | |
| **9.2** Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible. | **9.2.a** Review processes and procedures for assigning badges to onsite personnel and visitors, and verify these processes include the following:<br>▪ Granting new badges,<br>▪ Changing access requirements, and<br>▪ Revoking terminated onsite personnel and expired visitor badges | | | |
| | **9.2.b** Verify that access to the badge system is limited to authorized personnel. | | | |
| | **9.2.c** Examine badges in use to verify that they clearly identify visitors and it is easy to distinguish between onsite personnel and visitors. | | | |
| **9.3** Make sure all visitors are handled as follows: | **9.3** Verify that visitor controls are in place as follows: | | | |
| **9.3.1** Authorized before entering areas where cardholder data is processed or maintained. | **9.3.1** Observe the use of visitor ID badges to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data. | | | |
| **9.3.2** Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel. | **9.3.2.a** Observe people within the facility to verify the use of visitor ID badges, and that visitors are easily distinguishable from onsite personnel. | | | |
| | **9.3.2.b** Verify that visitor badges expire. | | | |
| **9.3.3** Asked to surrender the physical token before leaving the facility or at the date of expiration. | **9.3.3** Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **9.4** Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law. | **9.4.a** Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted. | | | |
| | **9.4.b** Verify that the log contains the visitor's name, the firm represented, and the onsite personnel authorizing physical access, and is retained for at least three months. | | | |
| **9.5** Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually. | **9.5.a** Observe the storage location's physical security to confirm that backup media storage is secure. | | | |
| | **9.5.b** Verify that the storage location security is reviewed at least annually. | | | |
| **9.6** Physically secure all media. | **9.6** Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes). | | | |
| **9.7** Maintain strict control over the internal or external distribution of any kind of media, including the following: | **9.7** Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals. | | | |
| **9.7.1** Classify media so the sensitivity of the data can be determined. | **9.7.1** Verify that all media is classified so the sensitivity of the data can be determined. | | | |
| **9.7.2** Send the media by secured courier or other delivery method that can be accurately tracked. | **9.7.2** Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery method that can be tracked. | | | |
| **9.8** Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals). | **9.8** Select a recent sample of several days of offsite tracking logs for all media, and verify the presence in the logs of tracking details and proper management authorization. | | | |
| **9.9** Maintain strict control over the storage and accessibility of media. | **9.9** Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories. | | | |
| **9.9.1** Properly maintain inventory logs of all media and conduct media inventories at least annually. | **9.9.1** Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **9.10** Destroy media when it is no longer needed for business or legal reasons as follows: | **9.10** Obtain and examine the periodic media destruction policy and verify that it covers all media, and confirm the following: | | | |
| **9.10.1** Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed. | **9.10.1.a** Verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. | | | |
| | **9.10.1.b** Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a "to-be-shredded" container has a lock preventing access to its contents. | | | |
| **9.10.2** Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed. | **9.10.2** Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing). | | | |

## Regularly Monitor and Test Networks

### *Requirement 10: Track and monitor all access to network resources and cardholder data*

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **10.1** Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user. | **10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active for system components. | | | |
| **10.2** Implement automated audit trails for all system components to reconstruct the following events: | **10.2** Through interviews, examination of audit logs, and examination of audit log settings, perform the following: | | | |
| **10.2.1** All individual accesses to cardholder data | **10.2.1** Verify all individual access to cardholder data is logged. | | | |
| **10.2.2** All actions taken by any individual with root or administrative privileges | **10.2.2** Verify actions taken by any individual with root or administrative privileges are logged. | | | |
| **10.2.3** Access to all audit trails | **10.2.3** Verify access to all audit trails is logged. | | | |
| **10.2.4** Invalid logical access attempts | **10.2.4** Verify invalid logical access attempts are logged. | | | |
| **10.2 5** Use of identification and authentication mechanisms | **10.2.5** Verify use of identification and authentication mechanisms is logged. | | | |
| **10.2.6** Initialization of the audit logs | **10.2.6** Verify initialization of audit logs is logged. | | | |
| **10.2.7** Creation and deletion of system-level objects | **10.2.7** Verify creation and deletion of system level objects are logged. | | | |
| **10.3** Record at least the following audit trail entries for all system components for each event: | **10.3** Through interviews and observation, for each auditable event (from 10.2), perform the following: | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **10.3.1** User identification | **10.3.1** Verify user identification is included in log entries. | | | |
| **10.3.2** Type of event | **10.3.2** Verify type of event is included in log entries. | | | |
| **10.3.3** Date and time | **10.3.3** Verify date and time stamp is included in log entries. | | | |
| **10.3.4** Success or failure indication | **10.3.4** Verify success or failure indication is included in log entries. | | | |
| **10.3.5** Origination of event | **10.3.5** Verify origination of event is included in log entries. | | | |
| **10.3.6** Identity or name of affected data, system component, or resource. | **10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries. | | | |
| **10.4** Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.<br>***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).* | **10.4.a** Verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2. | | | |
| | **10.4.b** Obtain and review the process for acquiring, distributing and storing the correct time within the organization, and review the time-related system-parameter settings for a sample of system components. Verify the following is included in the process and implemented: | | | |
| **10.4.1** Critical systems have the correct and consistent time. | **10.4.1.a** Verify that only designated central time servers receive time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. | | | |
| | **10.4.1.b** Verify that the designated central time servers peer with each other to keep accurate time, and other internal servers receive time only from the central time servers. | | | |
| **10.4.2** Time data is protected. | **10.4.2.a** Review system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data. | | | |
| | **10.4.2.b** Review system configurations and time synchronization settings and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **10.4.3** Time settings are received from industry-accepted time sources. | **10.4.3** Verify that the time servers accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers). | | | |
| **10.5** Secure audit trails so they cannot be altered. | **10.5** Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows: | | | |
| **10.5.1** Limit viewing of audit trails to those with a job-related need. | **10.5.1** Verify that only individuals who have a job-related need can view audit trail files. | | | |
| **10.5.2** Protect audit trail files from unauthorized modifications. | **10.5.2** Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation. | | | |
| **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | **10.5.3** Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter. | | | |
| **10.5.4** Write logs for external-facing technologies onto a log server on the internal LAN. | **10.5.4** Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media. | | | |
| **10.5.5** Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). | **10.5.5** Verify the use of file-integrity monitoring or change-detection software for logs by examining system settings and monitored files and results from monitoring activities. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **10.6** Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).<br>***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.* | **10.6.a** Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required. | | | |
| | **10.6.b** Through observation and interviews, verify that regular log reviews are performed for all system components. | | | |
| **10.7** Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up). | **10.7.a** Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year. | | | |
| | **10.7.b** Verify that audit logs are available for at least one year and processes are in place to immediately restore at least the last three months' logs for analysis. | | | |

## Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **11.1** Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.<br>***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.*<br>*Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.* | **11.1.a** Verify that the entity has a documented process to detect and identify wireless access points on a quarterly basis. | | | |
| | **11.1.b** Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:<br>▪ WLAN cards inserted into system components<br>▪ Portable wireless devices connected to system components (for example, by USB, etc.)<br>▪ Wireless devices attached to a network port or network device | | | |
| | **11.1.c** Verify that the documented process to identify unauthorized wireless access points is performed at least quarterly for all system components and facilities. | | | |
| | **11.1.d** If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel. | | | |
| | **11.1.e** Verify the organization's incident response plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **11.2** Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).<br>***Note:*** *It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.* | **11.2** Verify that internal and external vulnerability scans are performed as follows: | | | |
| **11.2.1** Perform quarterly internal vulnerability scans. | **11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. | | | |
| | **11.2.1.b** Review the scan reports and verify that the scan process includes rescans until passing results are obtained, or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved. | | | |
| | **11.2.1.c** Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **11.2.2** Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).<br>***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by internal staff.* | **11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly scans occurred in the most recent 12-month period. | | | |
| | **11.2.2.b** Review the results of each quarterly scan to ensure that they satisfy the ASV Program Guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures). | | | |
| | **11.2.2.c** Review the scan reports to verify that the scans were completed by an Approved Scanning Vendor (ASV), approved by the PCI SSC. | | | |
| **11.2.3** Perform internal and external scans after any significant change.<br>***Note:*** *Scans conducted after changes may be performed by internal staff.* | **11.2.3.a** Inspect change control documentation and scan reports to verify that system components subject to any significant change were scanned. | | | |
| | **11.2.3.b** Review scan reports and verify that the scan process includes rescans until:<br>▪ For external scans, no vulnerabilities exist that are scored greater than a 4.0 by the CVSS,<br>▪ For internal scans, a passing result is obtained or all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved. | | | |
| | **11.2.3.c** Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **11.3** Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following: | **11.3.a** Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. | | | |
| | **11.3.b** Verify that noted exploitable vulnerabilities were corrected and testing repeated. | | | |
| | **11.3.c** Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). | | | |
| **11.3.1** Network-layer penetration tests | **11.3.1** Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operating systems. | | | |
| **11.3.2** Application-layer penetration tests | **11.3.2** Verify that the penetration test includes application-layer penetration tests. The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5. | | | |
| **11.4** Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises.<br>Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date. | **11.4.a** Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored. | | | |
| | **11.4.b** Confirm IDS and/or IPS are configured to alert personnel of suspected compromises. | | | |
| | **11.4.c** Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **11.5** Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.<br>***Note:** For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).* | **11.5.a** Verify the use of file-integrity monitoring tools within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities.<br>Examples of files that should be monitored:<br>▪ System executables<br>▪ Application executables<br>▪ Configuration and parameter files<br>▪ Centrally stored, historical or archived, log and audit files | | | |
| | **11.5.b** Verify the tools are configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly. | | | |

## Maintain an Information Security Policy

### *Requirement 12: Maintain a policy that addresses information security for all personnel.*

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **12.1** Establish, publish, maintain, and disseminate a security policy that accomplishes the following: | **12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners). | | | |
| **12.1.1** Addresses all PCI DSS requirements. | **12.1.1** Verify that the policy addresses all PCI DSS requirements. | | | |
| **12.1.2** Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.<br>(Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.) | **12.1.2.a** Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment. | | | |
| | **12.1.2.b** Review risk assessment documentation to verify that the risk assessment process is performed at least annually. | | | |
| **12.1.3** Includes a review at least annually and updates when the environment changes. | **12.1.3** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. | | | |
| **12.2** Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures). | **12.2** Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **12.3** Develop usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. Ensure these usage policies require the following: | **12.3** Obtain and examine the usage policies for critical technologies and perform the following: | | | |
| **12.3.1** Explicit approval by authorized parties | **12.3.1** Verify that the usage policies require explicit approval from authorized parties to use the technologies. | | | |
| **12.3.2** Authentication for use of the technology | **12.3.2** Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (for example, token). | | | |
| **12.3.3** A list of all such devices and personnel with access | **12.3.3** Verify that the usage policies require a list of all devices and personnel authorized to use the devices. | | | |
| **12.3.4** Labeling of devices to determine owner, contact information and purpose | **12.3.4** Verify that the usage policies require labeling of devices with information that can be correlated to owner, contact information and purpose. | | | |
| **12.3.5** Acceptable uses of the technology | **12.3.5** Verify that the usage policies require acceptable uses for the technology. | | | |
| **12.3.6** Acceptable network locations for the technologies | **12.3.6** Verify that the usage policies require acceptable network locations for the technology. | | | |
| **12.3.7** List of company-approved products | **12.3.7** Verify that the usage policies require a list of company-approved products. | | | |
| **12.3.8** Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity | **12.3.8** Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. | | | |
| **12.3.9** Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use | **12.3.9** Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **12.3.10** For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. | **12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. | | | |
| | **12.3.10.b** For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements. | | | |
| **12.4** Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. | **12.4** Verify that information security policies clearly define information security responsibilities for all personnel. | | | |
| **12.5** Assign to an individual or team the following information security management responsibilities: | **12.5** Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management.<br>Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned: | | | |
| **12.5.1** Establish, document, and distribute security policies and procedures. | **12.5.1** Verify that responsibility for creating and distributing security policies and procedures is formally assigned. | | | |
| **12.5.2** Monitor and analyze security alerts and information, and distribute to appropriate personnel. | **12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned. | | | |
| **12.5.3** Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. | **12.5.3** Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned. | | | |
| **12.5.4** Administer user accounts, including additions, deletions, and modifications | **12.5.4** Verify that responsibility for administering user account and authentication management is formally assigned. | | | |
| **12.5.5** Monitor and control all access to data. | **12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **12.6** Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. | **12.6.a** Verify the existence of a formal security awareness program for all personnel. | | | |
| | **12.6.b** Obtain and examine security awareness program procedures and documentation and perform the following: | | | |
| **12.6.1** Educate personnel upon hire and at least annually.<br>***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data..* | **12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions). | | | |
| | **12.6.1.b** Verify that personnel attend awareness training upon hire and at least annually. | | | |
| **12.6.2** Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures. | **12.6.2** Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy. | | | |
| **12.7** Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)<br>***Note:*** *For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.* | **12.7** Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on potential personnel prior to hire who will have access to cardholder data or the cardholder data environment. | | | |
| **12.8** If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following: | **12.8** If the entity shares cardholder data with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), through observation, review of policies and procedures, and review of supporting documentation, perform the following: | | | |
| **12.8.1** Maintain a list of service providers. | **12.8.1** Verify that a list of service providers is maintained. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **12.8.2** Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess. | **12.8.2** Verify that the written agreement includes an acknowledgement by the service providers of their responsibility for securing cardholder data. | | | |
| **12.8.3** Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. | **12.8.3** Verify that policies and procedures are documented and were followed including proper due diligence prior to engaging any service provider. | | | |
| **12.8.4** Maintain a program to monitor service providers' PCI DSS compliance status at least annually. | **12.8.4** Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually. | | | |
| **12.9** Implement an incident response plan. Be prepared to respond immediately to a system breach. | **12.9** Obtain and examine the Incident Response Plan and related procedures and perform the following: | | | |
| **12.9.1** Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:<br>▪ Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum<br>▪ Specific incident response procedures<br>▪ Business recovery and continuity procedures<br>▪ Data back-up processes<br>▪ Analysis of legal requirements for reporting compromises<br>▪ Coverage and responses of all critical system components<br>▪ Reference or inclusion of incident response procedures from the payment brands | **12.9.1.a** Verify that the incident response plan includes:<br>▪ Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum:<br>▪ Specific incident response procedures<br>▪ Business recovery and continuity procedures<br>▪ Data back-up processes<br>▪ Analysis of legal requirements for reporting compromises (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database)<br>▪ Coverage and responses for all critical system components<br>▪ Reference or inclusion of incident response procedures from the payment brands | | | |
| | **12.9.1.b** Review documentation from a previously reported incident or alert to verify that the documented incident response plan and procedures were followed. | | | |

| PCI DSS Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **12.9.2** Test the plan at least annually. | **12.9.2** Verify that the plan is tested at least annually. | | | |
| **12.9.3** Designate specific personnel to be available on a 24/7 basis to respond to alerts. | **12.9.3** Verify through observation and review of policies, that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes. | | | |
| **12.9.4** Provide appropriate training to staff with security breach response responsibilities. | **12.9.4** Verify through observation and review of policies that staff with responsibilities for security breach response are periodically trained. | | | |
| **12.9.5** Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems. | **12.9.5** Verify through observation and review of processes that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan. | | | |
| **12.9.6** Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | **12.9.6** Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | | | |

# Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

## *Requirement A.1: Shared hosting providers must protect the cardholder data environment*

As referenced in Requirement 12.8, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.

| Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **A.1** Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4:<br>A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.<br>***Note:*** *Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.* | **A.1** Specifically for a PCI DSS assessment of a shared hosting provider, to verify that shared hosting providers protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and perform A.1.1 through A.1.4 below: | | | |
| **A.1.1** Ensure that each entity only runs processes that have access to that entity's cardholder data environment. | **A.1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example:<br>No entity on the system can use a shared web server user ID.<br>All CGI scripts used by an entity must be created and run as the entity's unique user ID. | | | |

| Requirements | Testing Procedures | In Place | Not in Place | Target Date/ Comments |
|---|---|---|---|---|
| **A.1.2** Restrict each entity's access and privileges to its own cardholder data environment only. | **A.1.2.a** Verify the user ID of any application process is not a privileged user (root/admin). | | | |
| | **A.1.2.b** Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.)<br>**Important:** An entity's files may not be shared by group. | | | |
| | **A.1.2.c** Verify that an entity's users do not have write access to shared system binaries. | | | |
| | **A.1.2.d** Verify that viewing of log entries is restricted to the owning entity. | | | |
| | **A.1.2.e** To ensure each entity cannot monopolize server resources to exploit vulnerabilities (for example, error, race, and restart conditions, resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources:<br>▪ Disk space<br>▪ Bandwidth<br>▪ Memory<br>▪ CPU | | | |
| **A.1.3** Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10. | **A.1.3** Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment:<br>Logs are enabled for common third-party applications.<br>Logs are active by default.<br>Logs are available for review by the owning entity.<br>Log locations are clearly communicated to the owning entity. | | | |
| **A.1.4** Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. | **A.1.4** Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise. | | | |

# Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Navigating PCI DSS* for the intent of each PCI DSS requirement.)
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

   When evaluating "above and beyond" for compensating controls, consider the following:

***Note:** The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.*

   a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

   b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review. For example, two-factor authentication is a PCI DSS requirement for remote access. Two-factor authentication *from within the internal network* can also be considered as a compensating control for non-console administrative access when transmission of encrypted passwords cannot be supported. Two-factor authentication may be an acceptable compensating control if: (1) it meets the intent of the original requirement by addressing the risk of intercepting clear-text administrative passwords; and (2) it is set up properly and in a secure environment.

   c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per Requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) two-factor authentication from within the internal network.

4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

# Appendix C: Compensating Controls Worksheet

*Use this worksheet to define compensating controls for any requirement where compensating controls are used to meet a PCI DSS requirement. Note that compensating controls should also be documented in the Report on Compliance in the corresponding PCI DSS requirement section.*

***Note:*** *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

**Requirement Number and Definition:**

| | Information Required | Explanation |
|---|---|---|
| **1. Constraints** | List constraints precluding compliance with the original requirement. | |
| **2. Objective** | Define the objective of the original control; identify the objective met by the compensating control. | |
| **3. Identified Risk** | Identify any additional risk posed by the lack of the original control. | |
| **4. Definition of Compensating Controls** | Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any. | |
| **5. Validation of Compensating Controls** | Define how the compensating controls were validated and tested. | |
| **6. Maintenance** | Define process and controls in place to maintain compensating controls. | |

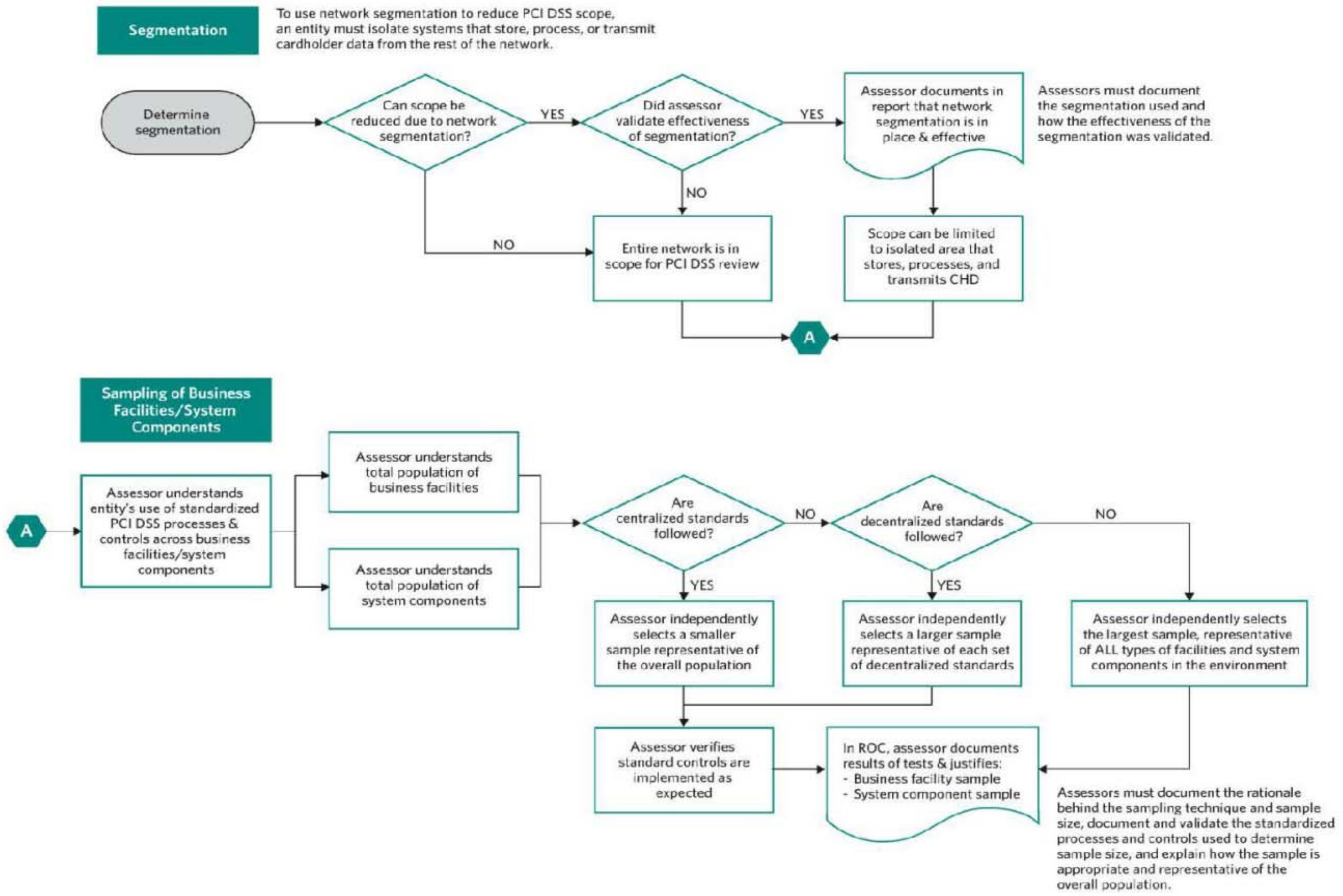
## Compensating Controls Worksheet – Completed Example

*Use this worksheet to define compensating controls for any requirement noted as "in place" via compensating controls.*

**Requirement Number:** *8.1—Are all users identified with a unique user name before allowing them to access system components or cardholder data?*

| | Information Required | Explanation |
|---|---|---|
| **1. Constraints** | List constraints precluding compliance with the original requirement. | *Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a "root" login. It is not possible for Company XYZ to manage the "root" login nor is it feasible to log all "root" activity by each user.* |
| **2. Objective** | Define the objective of the original control; identify the objective met by the compensating control. | *The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.* |
| **3. Identified Risk** | Identify any additional risk posed by the lack of the original control. | *Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.* |
| **4. Definition of Compensating Controls** | Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any. | *Company XYZ is going to require all users to log into the servers from their desktops using the SU command. SU allows a user to access the "root" account and perform actions under the "root" account but is able to be logged in the SU-log directory. In this way, each user's actions can be tracked through the SU account.* |
| **5. Validation of Compensating Controls** | Define how the compensating controls were validated and tested. | *Company XYZ demonstrates to assessor that the SU command being executed and that those individuals utilizing the command are logged to identify that the individual is performing actions under root privileges.* |
| **6. Maintenance** | Define process and controls in place to maintain compensating controls. | *Company XYZ documents processes and procedures to ensure SU configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually tracked or logged.* |

# Appendix D: Segmentation and Sampling of Business Facilities/System Components


Segmentation
To use network segmentation to reduce PCI DSS scope, an entity must isolate systems that store, process, or transmit cardholder data from the rest of the network.
Determine segmentation
Can scope be reduced due to network segmentation?
YES
NO
Did assessor validate effectiveness of segmentation?
YES
NO
Assessor documents in report that network segmentation is in place & effective
Assessors must document the segmentation used and how the effectiveness of the segmentation was validated.
Entire network is in scope for PCI DSS review
Scope can be limited to isolated area that stores, processes, and transmits CHD
A
Sampling of Business Facilities/System Components
A
Assessor understands entity's use of standardized PCI DSS processes & controls across business facilities/system components
Assessor understands total population of business facilities
Assessor understands total population of system components
Are centralized standards followed?
NO
YES
Are decentralized standards followed?
NO
YES
Assessor independently selects a smaller sample representative of the overall population
Assessor independently selects a larger sample representative of each set of decentralized standards
Assessor independently selects the largest sample, representative of ALL types of facilities and system components in the environment
Assessor verifies standard controls are implemented as expected
In ROC, assessor documents results of tests & justifies:
- Business facility sample
- System component sample
Assessors must document the rationale behind the sampling technique and sample size, document and validate the standardized processes and controls used to determine sample size, and explain how the sample is appropriate and representative of the overall population.

**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 __44__ 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 is intentionally left blank.**

**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF ARIZONA**

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

**LODGED UNDER SEAL**

**FTC PROPOSED EXHIBIT __61__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

BAIRD, WILLIAMS & GREER, L.L.P.
6225 NORTH 24TH STREET, SUITE 125
PHOENIX, ARIZONA 85016
TELEPHONE (602) 256-9400

Michael C. Blair (018994)
mblair@bwglaw.net
Attorneys for plaintiff

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

| | |
|---|---|
| Michael D. Peters, a married man,<br>Plaintiff, | No. |
| | **Complaint** |
| vs. | 1. Whistleblower Protection Pursuant to Sarbanes-Oxley Act, 18 U.S.C. § 1514A; |
| LifeLock, Inc., a Delaware corporation; Kim Jones, an Ohio citizen; Cristy Schaan, an Arizona citizen, | 2. Whistleblower Protection Pursuant to Dodd-Frank Act, 15 U.S.C. § 78u-6(h); |
| Defendants. | 3. Defamation |
| | **(Jury Trial Demanded)** |

For his complaint against defendants, plaintiff alleges as follows:

## - Jurisdiction and Venue -

1. This action against defendant LifeLock, Inc., arises under the whistleblower protection provisions of the Sarbanes-Oxley Act, 18 U.S.C. § 1514A, and the Dodd-Frank Act, 15 U.S.C. § 78u-6(h)(1)(A). This court has subject matter jurisdiction pursuant to 18 U.S.C. § 1514A(b)(1)(B) and 28 U.S.C. § 1331.

2. This action against defendants Kim Jones and Cristy Schaan seeks relief for Arizona state law claims for defamation. This court has supplemental jurisdiction over these claims pursuant to 28 U.S.C. § 1367(a).

3. Venue is proper pursuant to 18 U.S.C. § 1514A(b)(1)(B) and 28 U.S.C. § 1391(b) because the events described herein occurred within this district.

**- Parties -**

4. Plaintiff Michael D. Peters is a married man who is a citizen of Arizona.

5. Peters is an internationally recognized authority on information technology security. He has published numerous books and articles on the subject and has been a keynote speaker at several security conferences throughout the United States and overseas.

6. Peters is a member of the Information Systems Security Association (ISSA) Hall of Fame. Only 42 people in the world have been inducted. He was inducted for demonstrating a superior level of expertise, effectiveness, and dedication to the advancement of the cyber security profession. Peters is also a fellow at the ISSA. This is reserved for only 2% of all international members based on their contributions to the cyber security profession. Peters is also certified as a Chief Information Security Officer, as an Information System Security Professional, as an Information Security Manager, as a Computer Examiner, and in Risk and Information Systems Control.

7. Defendant LifeLock, Inc., is a Delaware corporation headquartered in Tempe, Arizona.

8. Defendant Kim Jones is a citizen of Ohio.

9. Defendant Cristy Schaan is a citizen of Arizona.

**- Demand for Jury Trial -**

10. Peters demands a jury trial pursuant to 18 U.S.C. § 1514A(b)(2)(E).

**- Factual Background -**

11. In early 2013, Peters was working as the Chief Information Security Officer ("CISO") for CrossView, Inc., in Midland, Georgia. He was contacted by a recruiter looking to fill a CISO position at LifeLock. Peters was intrigued with this opportunity so he decided to pursue it.

12. What followed was an intense screening and vetting process by LifeLock. This included more than twelve face-to-face interviews, numerous telephonic interviews, drug testing, a thorough review of eight years of Peters's tax returns, thorough criminal and civil background

checks, and background checks on his education and employment. Indeed, the screening process LifeLock used was more detailed and invasive than when Peters obtained a secret clearance from the United States Air Force. All checks and testing resulted in a clear or satisfactory result.

13. LifeLock offered Peters the position of CISO on May 23, 2013. He accepted the position on May 24. The offer was contingent upon the successful completion of background checks and drug testing. A third party, TalentWise, performed those background checks and drug testing for LifeLock. Peters successfully passed them on May 17 and May 30, respectively.

14. Peters was to be paid an annual base salary of $180,000.00 plus benefits and a stock option grant of 35,000 shares. Peters also had the opportunity to receive an annual bonus of up to 25% of his base salary.

15. In reliance upon LifeLock's offer, Peters resigned from his job in Georgia, sold his home there at a loss, forfeited prepaid tuition for private schools for his children, and then uprooted his family and moved to Arizona, a place where they had no family and knew no one.

16. Peters started work on July 1, 2013, as LifeLock's CISO.

17. Upon commencing work, Peters immediately began an initial risk assessment at LifeLock. Before his hiring, LifeLock had never conducted a bona fide risk assessment. Even in the preliminary stages of the risk assessment, Peters began to discover many instances of illegal and incompetent practices that constituted fraud against LifeLock's shareholders. These include, but are not limited to, the following:

a. LifeLock's manager of database administration, Jacqueline Hufford-Jensen, signed a Sarbanes-Oxley audit verifying that the information contained in that audit was true and correct even though the time period she was attesting to predated her hiring date at LifeLock.

b. LifeLock's director of internal audits, Tony Valentine, had "collected" evidence from the information security team that existed prior to Peters's arrival related to access logging, audit logging, audit log reviews, network security controls, and data leakage controls that either (1) did not truly exist because the technology was still in boxes; or (2) LifeLock lacked the staff to keep track of everything; or (3) such reviews were not actually conducted.

c. LifeLock employee Dave Bridgman told Peters that LifeLock's current practice was to manipulate the customer alerts sent to its elderly customers. LifeLock would turn off or reduce the services alerting elderly customers to reduce the call volume received by LifeLock's customer support center. Peters believed this was fraudulent since it sold its services to the general public without any disclosure that alert services would be limited for certain segments of the population.

d. LifeLock was in the process of finalizing a new product offering called PassLock. This system was designed to allow customers to include their passwords for up to ten accounts. PassLock would then crawl through hundreds of internet sites to check the username and password supplied by the customer and report back to the customer. The problem was that the database was not being protected with industry-grade encryption. The database was predicted to contain millions of customer credentials that would be devastating to consumers if a breach occurred. Moreover, the system was going to utilize a third-party cloud hosting business without that third party's knowledge or consent. Technically, the PassLock crawling would be identified by most service providers as intrusive, illegal, illegitimate, and then blacklist the source address. The unknowing third-party cloud hosting service would suffer significant business damage and LifeLock could face significant liability thereby damaging its shareholders.

18. LifeLock's security posture was at high risk. Peters determined that LifeLock's internal capacity for governance implemented (policies, audit plan, change controls, architectural review, etc.) was at 47% of the minimum to protect LifeLock's customers and their sensitive information. If a security breach occurred, LifeLock's shareholders would be damaged.

19. Peters determined that LifeLock's technological security readiness (intrusion prevention, data leakage, data encryption, access controls, physical security, etc.) was only at 27% of the minimum to protect LifeLock's customers and their sensitive information. If a security breach occurred, LifeLock's shareholders would be damaged.

20. Peters determined that LifeLock's security vigilance (vulnerability testing, auditing, monitoring, awareness education, event logging, incident management, etc.) was at 0% of the minimum to protect LifeLock's customers and their sensitive information. If a security breach occurred, LifeLock's shareholders would be damaged.

21. A large part of this problem was staffing. LifeLock only had two people responsible for security. One individual lacked technical skill and only had minimal security experience; the other was fresh out of college and had technical skills, but lacked experience if a data breach occurred. Peters concluded that millions of customers were at risk given the data LifeLock possesses and is incapable of protecting.

22. Peters asked LifeLock to immediately hire at least 12 information security professionals to get LifeLock to the minimum level necessary for basic information security protection. LifeLock said it might hire two people during the next 12 months, but full staffing would take years, if at all.

23. On or about July 9, 2013, Peters met with LifeLock's CFO, Chris Power. Peters advised Power of what he was discovering as part of his ongoing initial risk assessment described in paragraphs 17–21 above. Power did nothing in response.

24. On or about July 12, 2013, Peters met with his direct superior, LifeLock's chief information officer, Rich Stebbins. Peters advised Stebbins of what he was discovering as part of his ongoing initial risk assessment described in paragraphs 17–21 above. Stebbins did nothing in response.

25. LifeLock's upper management decided to fire Peters after he met with Power and Stebbins and conveyed to them the preliminary results of his ongoing initial risk assessment.

26. LifeLock's upper management directed Michelle Deutsch, LifeLock's in-house special counsel for labor and employment, to try to find grounds to terminate Peters's employment at LifeLock.

27. In mid-July 2013, Deutsch contacted CrossView, Inc., about Peters's work there. Deutsch also contacted another of Peters's former employers, Fifth Third Processing Solutions, now known as Vantiv, in Ohio.

28. When Deutsch contacted Vantiv, she was incorrectly told that Peters had been fired. This was and is a false statement. Peters resigned from Fifth Third Processing Solutions pursuant to a signed separation agreement.

29. On his employment application with LifeLock, Peters stated that he resigned from Fifth Third Processing Solutions and moved to Georgia with his U.S. Army wife to keep his family together. This statement is true because his family did, in fact, move to Georgia and, pursuant to the separation agreement with Fifth Third Processing Solutions, he had resigned from that entity.

30. Based on the false information Deutsch obtained from Vantiv, LifeLock decided it had cause to terminate Peters by claiming that he made a misrepresentation on his employment application regarding his departure from Fifth Third Processing Solutions.

31. LifeLock fired Peters on July 29, 2013.

32. Peters wrote a letter to LifeLock's CEO, Todd Davis, on July 30 to try to get his job back. It did not happen. Instead, on August 1, LifeLock's attorney sent a letter to Peters advising that he had been terminated for cause because of false information on his employment application.

### - Administrative Actions -

33. Peters filed a complaint with the FTC against LifeLock on August 19, 2013. That complaint is still under investigation.

34. Peters filed a complaint with the SEC against LifeLock on August 19, 2013. That complaint is still under investigation.

35. Peters filed a whistleblower complaint with the U.S. Department of Labor under the Sarbanes-Oxley Act on August 23, 2013, against LifeLock and Vantiv. OSHA investigates

Sarbanes-Oxley complaints. An OSHA mediator resolved the complaint between Peters and Vantiv. A signed settlement agreement was entered between Peters and Vantiv on September 27, 2013.

36. The Sarbanes-Oxley complaint against LifeLock was still active. However, more than 180 days has passed since the filing of the complaint so, on February 25, 2014, Peters notified OSHA of his intent to file suit in district court.

**Count I - Violation of Whistleblower Provisions of Sarbanes-Oxley Act Against LifeLock**

37. Peters incorporates paragraphs 1–36 contained herein.

**- Peters Engaged In Protected Activity -**

38. While conducting his initial risk assessment, and based on his extensive experience and training in the information technology security world, Peters both subjectively and objectively believed that LifeLock was committing fraud against its shareholders as described in paragraphs 17–21, *supra.*

**- Knowledge of Decision Maker -**

39. Peters disclosed the preliminary findings from his ongoing initial risk assessment to both Stebbins and Power, his supervisors, on separate occasions and conveyed to them his belief that LifeLock was engaging in fraudulent activities.

40. Stebbins and Power conveyed the information they received from Peters to other members of LifeLock's upper management so LifeLock's decision makers knew about Peters's preliminary findings from his ongoing initial risk assessment.

41. LifeLock's upper management decided that Peters had to be fired, so they tasked Deutsch to find a basis to do so.

**- Unfavorable Personnel Action -**

42. LifeLock fired Peters on July 29, 2013.

**- Contributing Factor -**

43. LifeLock conducted an exhaustive background search on Peters as part of its vetting process before offering him the job as its CISO. LifeLock even hired an outside third-party entity, TalentWise, to conduct background checks on Peters's education, employment, civil and criminal history, and drug testing.

44. TalentWise specifically contacted Fifth Third Processing Systems to verify Peters's employment there and the information he provided on his LifeLock application. TalentWise's employment check with Fifth Third Processing Solutions came back clear.

45. Notwithstanding the clean background checks, Deutsch started her own background check in mid-July immediately after Peters had his separate meetings with Stebbins and Power.

46. LifeLock had no reason to contact Peters's former employers in mid-July because TalentWise's background check on his employment had been completed in May before he was even hired. Nonetheless, Deutsch contacted an unknown individual at Vantiv and was given false information about Peters's employment at Fifth Third Processing Solutions. LifeLock believed this was sufficient to claim that Peters had provided false information on his employment application.

47. LifeLock fired Peters approximately two weeks after he reported the fraudulent conduct he was discovering during his initial risk assessment.

**- LifeLock's Pretextual Defense -**

48. LifeLock claims it fired Peters because of false information Deutsch obtained when she contacted Vantiv about Peters's employment at Fifth Third Processing Solutions. However, Vantiv has acknowledged that Peters was not fired, but that he resigned. Any alleged statements to the contrary are false. Deutsch never contacted Peters to get his side of the story. Instead, LifeLock used the false information Deutsch obtained as a pretext to fire him.

49. Peters learned through the OSHA investigation that defendant Cristy Schaan at LifeLock surreptitiously conducted her own private investigation of Peters's prior employment at Fifth Third Processing Solutions. Schaan was the interim CISO at LifeLock before Peters was hired. She applied for the permanent CISO position also, but was passed over in favor of Peters. On July 1, 2013, she contacted defendant Kim Jones, Vantiv's CISO, to find out what, if anything, he personally knew about Peters.

50. Jones stated that he did not know Peters. He said that Peters was the predecessor CISO to Jones's predecessor at Vantiv. Notwithstanding, Jones then proceeded to tell Schaan all sorts of false and negative things about Peters. Jones has since admitted that he did not contact anyone at Vantiv legal or Vantiv human resources because he did not want his comments to be construed as

an official Vantiv response to Schaan's inquiry. Nonetheless, he provided this defamatory hearsay information via email to Schaan. She kept this negative information to use against Peters at a future date if the opportunity arose.

51. When Schaan discovered that LifeLock was about to fire Peters, she contacted Stebbins on July 26 and provided the defamatory hearsay email from Jones to try to seal Peters's fate. Peters's termination just three days later opened the door for Schaan to become LifeLock's CISO.

52. Within thirty days after firing Peters, LifeLock hired Schaan as its new CISO.

53. LifeLock has also claimed in response to Peters's OSHA complaint that Peters was terminated for inappropriate behavior because he allegedly "hit upon" a female employee. That allegation is false. Furthermore, the employee who made that allegation was Jacqueline Hufford-Jensen, the same employee who signed the fraudulent Sarbanes-Oxley audit. Hufford-Jensen made these false allegations to get Peters fired to cover up her signing of the fraudulent audit.

54. LifeLock's purported reasons for terminating Peters based on allegedly false information on his application and alleged improper conduct towards Hufford-Jensen were just a pretext to cover up the real reason for his termination: that he reported to his supervisors about the illegal, fraudulent, and incompetent business practices relating to fraud against shareholders that were occurring at LifeLock.

55. As a protected whistleblower, and pursuant to 18 U.S.C. § 1514A(c), Peters is entitled to all relief necessary to make him whole.

Wherefore, Peters prays for entry of judgment against LifeLock as follows:

A. pursuant to 18 U.S.C. § 1514A(c)(2)(B), for an order awarding Peters his back pay at the agreed upon salary with interest at the highest rate allowable by law. Peters also seeks the value, as of July 1, 2013, of the 35,000 stock options and 25% bonus granted to him as part of his compensation package;

B. pursuant to 18 U.S.C. § 1514A(c)(2)(C), for an order awarding Peters the special damages he sustained due to LifeLock's termination of his employment. These special damages include, but are not limited to:

i. all costs and expenses in an amount to be determined at trial that Peters incurred in moving his family from Georgia to Arizona in reliance upon LifeLock's offer of employment. These include the loss Peters sustained when he sold his home in Georgia, the forfeiture of prepaid school tuition, and the actual moving expenses he incurred to physically move his family and belongings across the country;

ii. damages in an amount to be determined at trial due to the emotional harm and anxiety Peters has suffered after moving his family across the country only to be fired just 29 days into his new job;

iii. all damages to Peters's reputation in an amount to be determined at trial;

iv. all of Peters's litigation costs, expert witness fees, and reasonable attorney fees incurred herein;

C. for an award of interest on all amounts awarded at the highest rate allowable by law from the date of judgment until paid in full; and

D. for such further relief as this court deems appropriate.

**Count II - Violation of Whistleblower Provisions of Dodd-Frank Act Against LifeLock**

56. Peters hereby incorporates paragraphs 1–55 herein.

57. In mid-July 2013, Peters reported to both Stebbins and Power and others of the illegal and incompetent practices that constituted fraud against LifeLock's shareholders as described in paragraphs 17-21, *supra*.

58. As described herein, Peters was fired on July 29 after reporting to his superiors those illegal and incompetent practices that constituted fraud against LifeLock's shareholders.

59. Peters filed a complaint against LifeLock with the SEC on August 19, 2013.

60. Pursuant to 15 U.S.C. § 78u-6(h)(1)(A)(i) and (iii), Peters is a whistleblower. LifeLock's termination of Peters violates the Dodd-Frank Act's protection for whistleblowers.

Wherefore, Peters prays for entry of judgment against LifeLock as follow:

A. pursuant to 15 U.S.C. § 78u-6(h)(1)(C)(ii), for an order awarding Peters two times his back pay at the agreed upon salary with interest at the highest rate allowable by law. Peters also seeks the value, as of July 1, 2013, of two times the 35,000 stock options and 25% bonus granted to him as part of his compensation package;

B. pursuant to 15 U.S.C. § 78u-6(h)(1)(C)(iii) for an order awarding Peters all of his litigation costs, expert witness fees, and reasonable attorney fees incurred herein;

C. for an award of interest on all amounts awarded at the highest rate allowable by law from the date of judgment until paid in full; and

D. for such further relief as this court deems appropriate.

**Count III - Defamation Against Kim Jones**

61. Peters hereby incorporates paragraphs 1–60 herein.

62. On July 2, 2013, Jones sent an email to Schaan at LifeLock responding to her request for information about Peters.

63. Jones's July 2 email contains false information. Jones falsely stated that Peters was fired from Fifth Third Processing Solutions and that he was walked out of the building without being allowed to return to his office to retrieve his personal belongings. In fact, Peters resigned.

64. Jones's July 2 email contains defamatory statements that bring Peters into disrepute, contempt, or ridicule or that impeach his honesty, integrity, virtue, or reputation.

a. Jones described Peters's relationship building skills as being virtually non-existent;

b. Jones said that Peters has a reputation for being disingenuous in his promotional activities by overstating his accomplishments; and

c. Jones stated that Peters engaged in inappropriate actions.

65. Jones has since admitted that he did not know Peters when Schaan asked about him. Jones has also admitted that he deliberately did not request any information about Peters from Vantiv's legal or human resources departments because he did not want his response to be misconstrued as an official Vantiv communication. In responding to Schaan's request, Jones was acting outside the scope of his employment at Vantiv.

66. Jones acted in reckless disregard of the truth or falsity of the statements he made about Peters to Schaan because he consciously disregarded whether that information was true or false.

Instead of verifying the information, Jones relied upon community gossip and conveyed that to Schaan as if it were true.

67. Jones failed to use reasonable care in determining whether his statements about Peters were true or false when he sent his July 2 email to Schaan.

68. On July 26, 2013, Schaan provided Stebbins with Jones's July 2 email and conveyed its contents as being true. LifeLock considered Jones's July 2 email as part of the decision to terminate Peters.

Wherefore, Peters prays for entry of judgment against defendant Kim Jones as follows:

A. for an order awarding Peters damages in an amount to be determined at trial due to Jones's defamatory July 2 email. These damages include, but are not limited to:

i. Peters's loss of employment at LifeLock;

ii. Peters is known worldwide for his work in information technology security. He is among the top 1% of all followed profiles on the social network LinkedIn. Working at LifeLock for only 29 days has damaged Peters's reputation and standing in the community;

iii. Peters has suffered emotional distress, humiliation, inconvenience, and anxiety as a result of Jones's defamatory July 2 email; and

iv. all monetary losses Peters has experienced and those that are reasonably probable for him to experience in the future;

B. to the extent Jones acted consciously and with reckless disregard of the truth of the statements contained in his July 2 email, Peters seeks an award of punitive damages;

C. for an award of interest on all amounts awarded at the highest rate allowable by law from the date of judgment until paid in full; and

D. for such further relief as this court deems appropriate.

## Count IV - Defamation Against Cristy Schaan

69. Peters hereby incorporates paragraphs 1–68 herein.

70. As stated above, before Peters was hired as LifeLock's CISO, Schaan was the interim CISO. Much of the illegal and incompetent practices Peters discovered during his ongoing initial

risk assessment occurred while Schaan was interim CISO. She applied for the permanent position, but it was given to Peters. When Peters began work at LifeLock, Schaan reported to him.

71. On July 1, 2013, Schaan asked her friend, defendant Kim Jones, if he knew anything about Peters and his employment at Fifth Third Processing Solutions.

72. Jones responded on July 2 with the defamatory hearsay email described in paragraphs 61–68, *supra*.

73. Based on the content of Jones's July 2 email, Schaan knew or had reason to know that it was defamatory because it brought Peters into disrepute, contempt, or ridicule or it impeached his honesty, integrity, virtue, or reputation.

74. Schaan kept Jones's July 2 email to herself until the end of July when she found out that LifeLock was considering terminating Peters.

75. On July 26, 2013, Schaan gave Stebbins a copy of Jones's July 2 defamatory email.

76. Schaan acted in reckless disregard of the truth or falsity of the statements in Jones's email about Peters when she re-published his defamatory email to Stebbins because she consciously disregarded whether that information was true or false. Instead, she wanted Peters to get fired so she could be LifeLock's CISO.

77. Schaan failed to use reasonable care in determining whether the statements in Jones's July 2 email about Peters were true or false when she re-published his defamatory email to Stebbins.

78. When Schaan provided Stebbins with Jones's July 2 email, she conveyed its contents as being true. The information Schaan provided to Stebbins was considered by LifeLock as part of the decision to terminate Peters.

Wherefore, Peters prays for entry of judgment against defendant Cristy Schaan as follows:

A. for an order awarding Peters damages in an amount to be determined at trial due to Schaan's re-publication of Jones's defamatory July 2 email. These damages include, but are not limited to:

i. Peters's loss of employment at LifeLock;

ii. Peters is known worldwide for his work in information technology security. He is among the top 1% of all followed profiles on the social network

LinkedIn. Working at LifeLock for only 29 days has damaged Peters's reputation and standing in the community;

iii. Peters has suffered emotional distress, humiliation, inconvenience, and anxiety as a result of Schaan's re-publication of Jones's defamatory July 2 email; and

iv. all monetary losses Peters has experienced and those that are reasonably probable for him to experience in the future;

B. to the extent Schaan acted consciously and with reckless disregard of the truth of the statements contained in Jones's July 2 defamatory email when she republished it to Stebbins on July 26, Peters seeks an award of punitive damages;

C. for an award of interest on all amounts awarded at the highest rate allowable by law from the date of judgment until paid in full; and

D. for such further relief as this court deems appropriate.

Dated this 19th day of March 2014.

*/s/ Michael C. Blair*
Michael C. Blair
*Baird, Williams & Greer, LLP*
6225 North 24th Street, Suite 125
Phoenix, Arizona 85016
Attorneys for plaintiff

## UNITED STATES DISTRICT COURT
## DISTRICT OF ARIZONA

# Civil Cover Sheet

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

**The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.**

| | |
|---|---|
| **Plaintiff** (s): **Michael D Peters** | **Defendant** (s): **LifeLock, Inc. ; Kim Jones ; Cristy Schaan** |
| County of Residence: Maricopa | County of Residence: Outside the State of Arizona |
| County Where Claim For Relief Arose: Maricopa | |
| Plaintiff's Atty(s): | Defendant's Atty(s): |

**Michael C. Blair**
**Baird, Williams & Greer, L.L.P.**
**6225 N. 24th St., Suite 125**
**Phoenix, Arizona 85016**
**602-256-9400**

II. Basis of Jurisdiction: **3. Federal Question (U.S. not a party)**

III. Citizenship of Principal Parties **(Diversity Cases Only)**
Plaintiff:- **N/A**
Defendant:- **N/A**

IV. Origin : **1. Original Proceeding**

V. Nature of Suit: **890 Other Statutory Actions**

VI.Cause of Action: **Whistleblower protection pursuant to Sarbanes-Oxley, 18 U.S.C. § 1514A, and Dodd-Frank, 15 U.S.C. § 78u-6(h); state law claims for defamation**

VII. Requested in Complaint
Class Action: **No**

Dollar Demand:
Jury Demand: **Yes**

VIII. This case **is not related** to another case.

**Signature: Michael C. Blair**

**Date: 3/19/14**

**If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it. Once correct, save this form as a PDF and include it as an attachment to your case opening documents.**

**Revised: 01/2014**

**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF ARIZONA**

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

**LODGED UNDER SEAL**

**FTC PROPOSED EXHIBIT __66__ 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 is intentionally left blank.**

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

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

**LODGED UNDER SEAL**

**FTC PROPOSED EXHIBIT __72__ TO MEMORANDUM IN SUPPORT OF ITS MOTION FOR CONTEMPT AGAINST LIFELOCK, INC.**

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

**Bureau of Consumer Protection**
**Division of Enforcement**
600 Pennsylvania Ave., NW
Mailstop M-8102B
Washington, DC 20580

**Gregory J. Madden**
T: (202) 326-2426
E: gmadden@ftc.gov
F: (202) 326-2558

March 13, 2014

**Via FedEx and Email**
Andrew Berg, Esq.
Greenberg Traurig, LLP
2101 L Street N.W.
Washington, D.C. 20005
berga@gtlaw.com

Re: FTC v. LifeLock, Inc. et al, 10-CV-530 (D. Ariz.)

Mr. Berg:

Pursuant to Section VI., Compliance Monitoring, of the Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief as to Defendants LifeLock and Davis ("Stipulated Judgment") entered in the above referenced matter on March 15, 2010, the Federal Trade Commission ("FTC" or "Commission") is requesting information and documents related to the activities of LifeLock, Inc. ("LifeLock").

Specifically, the FTC requests that LifeLock respond to the specifications listed below. Please itemize your responses according to the numbered paragraphs in this letter. Please provide your written response and documentation within ten (10) business days of the receipt of this request.

**SPECIFICATIONS**

**LifeLock Alerts**

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

2. Describe each of the different types of "alerts" that LifeLock provides to LifeLock customers. Include within your description the sources(s) of information that generate each type of alert.

3. Describe all claims in any advertising or marketing regarding each and every type of alert that will be provided to LifeLock customers.

4. Describe any instances where LifeLock did not provide the alerts described in its advertising or marketing. Include within your description, the types of alerts, the number of alerts involved, the number of customers involved, and the dates of each instance.

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.

6. Describe what is encompassed by the "alert throttling" discussed in the LifeLock email communications in Attachment A, including the implementation, if any, of alert throttling. Include within your description, the types of alerts, the number of alerts involved, the number of customers involved, and the dates of each instance.

7. Describe any other "alert throttling" that LifeLock considered or implemented. Include within your description, the types of alerts, the number of alerts involved, the number of customers involved, and the dates of each instance.

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.

9. Explain what "PRD" means as discussed in Attachment A.

10. Provide the number of customer complaints, by type of alert, by month, where any customer complained that they did not receive an alert the customer believed he should have received from LifeLock.

**Information Security Program**

11. Describe LifeLock's internal organizational structure for its information security program safeguarding consumers' personal information ("personal information" as defined in the Stipulated Order) from October 2012 to present. Include within

your description the date of any changes to the internal organizational structure.

12. For the period October 2012 to present, describe the responsibilities and functions of each of the following groups identified on Attachment B, InfoSec Organization table:

    a. Governance, Risk, Compliance
    b. Security Operations
    c. Security Technology

13. For the period October 2012 to present, identify each of the groups in Specification No. 12.a-c, whose responsibilities and functions are related to LifeLock's information security program safeguarding consumers' personal information. For each group identified, describe how those responsibilities and functions relate to safeguarding consumers' personal information.

14. Identify all current or past employees, from October 2012 to present, whose job function is, or was, related to LifeLock's information security program for safeguarding consumers' personal information.

15. For each employee identified in response to Specification No. 14, provide:

    a. their job title(s) during the period October 2012 to present;
    b. the beginning and ending date for each job they held;
    c. where in the InfoSec Organization structure each job was located; and
    d. the functions related to LifeLock's information security program safeguarding consumers' personal information for each job.

16. For each job title for each employee identified in response to Specification No. 15.a, estimate the *percentage* of their time spent on job responsibilities involving information security management safeguarding consumers' personal information for each of the periods of time identified in Specification No. 15.b.

17. Identify all current or past employees, from October 2012 to present, whose *primary* job responsibility is, or was, related to LifeLock's information security program safeguarding consumers' personal information.

18. Identify and describe any internal or external information security risk assessments, draft or final, related to LifeLock's information security management safeguarding consumers' personal information conducted since October 2012 to present. Please include any assessments of:

    a. Employee training and management;
    b. Information systems;
    c. Prevention or detection of attacks, intrusions, or other systems failures, including vulnerability testing, auditing, monitoring, event logging,

awareness education, incident management; and

d. Responses to attacks, intrusions, or other systems failures.

19. Describe LifeLock's continuous monitoring activity for its information security program safeguarding consumers' personal information from October 2012 to the present.

20. Describe LifeLock's detection processes for its information security program safeguarding consumers' personal information from October 2012 to the present.

21. Identify and describe any attacks, intrusions, systems failures, or anomalous activity detection related to LifeLock's information security program safeguarding consumers' personal information from October 2012 to present.

22. Identify and describe any security breaches or incidents related to LifeLock's information security program safeguarding customers' personal information from October 2012 to present.

23. Describe any actions LifeLock undertook in response to any security breaches or incidents identified in response to Specification Nos. 21 and 22.

24. Identify and describe any certifications from outside third parties (e.g., ISO, NIST), from October 2012 to present, of LifeLock's information security program safeguarding consumers' personal information.

**LifeLock Wallet**

25. Describe how the "App Lock" feature on the LifeLock Wallet application protects a consumer's personal information if a consumer's mobile device is lost or stolen.

26. Describe how the App Lock feature works on a mobile device with the LifeLock Wallet application. Include in your description how the App Lock feature is enabled and disabled; what happens when the mobile device is turned on and off; what happens when the LifeLock Wallet application is opened and closed; and what happens to the App Lock feature in all other scenarios.

27. Produce the resumes or qualifications for each of the individuals identified in response to Specification No. 14.

28. Produce the job descriptions for each of the jobs identified in response to Specification No. 15, for the time period from October 2012 to the present.

29. Produce any internal or external security risk assessments, draft or final, related or referring to LifeLock's information security program safeguarding of consumers' personal information conducted from October 2012 to present.

30. Produce all documents relating or referring to any internal or external risk assessments of LifeLock's information security program safeguarding of consumers' personal information conducted from October 2012 to present.

31. To the extent not previously produced in response to the above document Request Specifications, produce all documentation supporting the information you have provided in response to Specification Nos. 10-24.

Please provide complete copies of all documents and information requested. If any document is undated, state the date on which it was prepared or received. Documents or other materials that are responsive to more than one specification do not need to be submitted more than once; however, you should indicate, on each item submitted, the specification number to which it corresponds.

Documents stored in hard copy should be submitted in an electronic format when at all possible. Please contact me to coordinate submission of Electronically Stored Information ("ESI"). Before submitting any electronic production, please confirm with me that the proposed formats and media types will be acceptable to the Commission. The FTC requests Concordance load-ready electronic productions, including DAT and OPT load files.

All claims for withholding information based on privilege (e.g., attorney-client, the Fifth Amendment) or judicial order must be asserted on or before compliance with this request. If any responsive material is withheld, please submit a schedule of the items withheld which states individually as to each such item the type, title, specific subject matter, and date of the item; the names, addresses, positions, and organizations of all authors and recipients of the item; and the specific grounds for claiming that the item is privileged.

We reserve the right to seek access to additional records and pursue such additional avenues of inquiry as are appropriate. Because the Commission may, at a later time, request all documents relating to any of the Specifications in this letter, please suspend any procedures for document destruction and take other measures to prevent the destruction of documents that are relevant to this investigation while it is pending.

Please swear or certify under penalty of perjury that the documents and other information produced or identified in response to this letter are complete and accurate and that the documents and information represent all documents and information responsive to this letter.

Please provide the requested documents and information by **March 31, 2014** to

David Hendrickson, Investigator
Federal Trade Commission
600 Pennsylvania Ave., NW, M-8102B
Washington, DC 20580

Telephone (202) 326-2107

We request that all materials be sent via overnight courier, such as FedEx, because U.S. Mail to the Federal Trade Commission is diverted and may be damaged in a security procedure.

If you have any questions, please contact me at (202) 326-2426. Your prompt cooperation and assistance is appreciated.

Sincerely,

Gregory J Madden

Gregory J. Madden