Consumer Remediation Plan
Communications Package

This document provides the consumer remediation communication plan in response to the potential for malicious code that could infect a customer's computer. This remediation communications package includes the following:

Table of Contents

Summary of Remediation Plan

We have created a consumer remediation plan in response to the potential for malicious code that could infect a customer's computer. This remediation communications package includes the following:

Consumer Notification

We recommend notifying consumers who may have been affected using the sample notification letter included in this package. This notification provides the conditions under which a customer is likely to have been affected, and the subsequent call to action directs them to a phone number where they will receive additional information about steps they need to take to ensure they are protected These steps include installing complimentary virus protection software to check their machine for infections, and signing up for complimentary credit monitoring. Details about these are listed below and later in this document.

You may choose to email customers directly using the information here, or CheckFree can email them on your behalf using a customized "from" address representing your company. If you would like CheckFree to notify consumers on your behalf via e-mail, please notify your CheckFree representative. In either case, please notify CheckFree of your plans to communicate with customers so that our call centers can be adequately staffed.

Call Experience for Consumers Who Need to Take Action

In the consumer notification, the call to action directs those with the potential to have been infected to a call center where they will be given further instructions. The details of what they will hear when the call this number are included in this package.

Complimentary Virus Protection

We will provide a one-year subscription for McAfee® VirusScan® Plus virus protection for those who were redirected, and either do not have any virus protection, or had an expired, out-of-date service. We will provide and administer this subscription at our expense.

Details about how a customer redeems this service, including screen shots, follow in this document. Your customers may activate this service at http://us.mcafee.com/root/campaign.asp?cid=53348 The code for redeeming this service is **VSPPROMOCF**. This code is valid through **December 31, 2008.**

Complimentary Credit Monitoring

We will provide a two-year subscription to Deluxe ID Theft Block Plus, a credit monitoring and identity theft protection service. We will provide and administer this service at our expense.

Details about how a customer redeems this service, including screen shots, follow in this document. Your customers may activate this service at http://www.deluxe-idtheftblock.com/secure by entering validation code **BR200804FI**. This code is valid through **December 31, 2008.**

Call Center FAQ

We have prepared our own customer call centers with an FAQ to address customer concerns which you may use with your call centers as well. This is included on pages.

Sample Customer Notification for Customers

From: %%Company_Name%% Customer Care
Sent: Friday, December 05, 2008 12:52 PM
To: <<CUSTOMER NAME>>
Subject: Important Information Regarding Your <<SERVICE NAME>> Bill Pay Service

Dear <<CUSTOMER NAME>>,

We take great care to keep your personal information secure. As part of these ongoing efforts, we are notifying you that the computer you use for online bill payment may be infected with malicious software that puts the security of your computer's contents at risk. This letter will help you determine if your computer is actually infected and advise you how to fix the problem and protect yourself against future risk.

The malicious software affects some but not all customers who accessed online bill payment on Tuesday, December 2, 2008. For a limited period of time, some customers were redirected from the authentic bill payment service to another site that may have installed malicious software. Your computer may be infected if all of the following are true:

- You attempted to access online bill payment between 12:30 a.m. and 10:10 a.m. Eastern time (GMT -5) on Tuesday, December 2, 2008, **and**
- You were using a computer with the Windows operating system, **and**
- You reached a blank screen rather than the usual bill payment screen when you attempted to navigate to online bill payment, **and**
- After reaching the blank screen, your computer's virus protection program did not tell you via pop-up or other messaging that malicious software was detected and quarantined.

If all four of the conditions above are true, your computer may be infected. We have arranged with McAfee, the world's largest dedicated security technology company, to provide you with an assessment of your computer's hard drive and remove any malicious software. Please contact us at 877-800-4864 for further instructions. We will also offer you both advice and free services that can help you mitigate any risk you may face as a result of this incident or other everyday exposures you may encounter.

We value your business and your trust, and we apologize for any inconvenience this recent incident has caused.

Thank you.

Call Experience for Consumers Who Need to Take Action

Line Greeting for 877-800-4864:

Thank you for calling Billpay support. My name is <<xxx>>. In order to provide you with the appropriate level of support, I would like to ask you a few general questions.

- Are you calling in response to an important notice email you received?

    NO: How may I direct your call?

    YES: (Move to next question).

- May I have your first name, last name, and zip code? (Document answers)

- May I have the email address where you received this particular email?

- (Document email address).

- Does your computer run on the Windows Operating System?

- Did you attempt to access the online bill payment site between 12:30 a.m. and 10:10 a.m. Eastern time (GMT -5) on Tuesday, December 2, 2008?

- Did you reach a blank screen rather than the usual bill payment screen when you attempted to access the online bill payment site?

- After you reached the blank screen, did your computer's virus protection program tell you that malicious software was detected and quarantined?
Note: Reconfirm with the customer that their virus protection software **did not** detect and quarantine the malicious software or they did not have such software.

(If the first 3 questions were YES and the final question was NO)

Based on your responses, we recommend you take the several precautionary steps that will be outlined in the email that I will send you which will include instructions for taking advantage of anti-virus software and identify protection software that we will provide at no cost to you.

Send email template to subscriber.

(If the first 3 questions were NO and the last question was YES – Confirmed YES)

Based on your answers of these questions, you were not impacted by this event. We apologize for the inconvenience this has caused.

If the subscriber asks a question that has not been addressed in the FAQs, ask the customer for their phone number for a call back. **

McAfee Installation Process

Refer to the McAfee site for a helpful FAQ with the top 10 consumer questions, including how to install and how to remove incompatible third party applications.
http://service.mcafee.com/FAQSearch.aspx

The following instructions detail the common path that consumers will follow to install McAfee and scan and repair their computers.
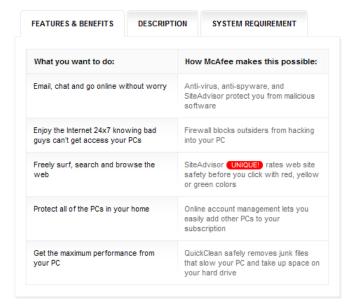
Instructions

1. Click the McAfee link in the e-mail received from your financial institution or CheckFree. **McAfee landing page appears with text about the December 2nd incident.**
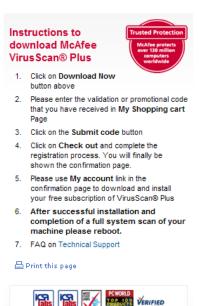2. Click the red Download Now button on the right side of the page.

CHECKFREE CONFIDENTIAL INFORMATION
Contains confidential and/or proprietary information of CheckFree. May only be used by or distributed to individuals specifically authorized by CheckFree.

© 2008 CheckFree Corporation.   5
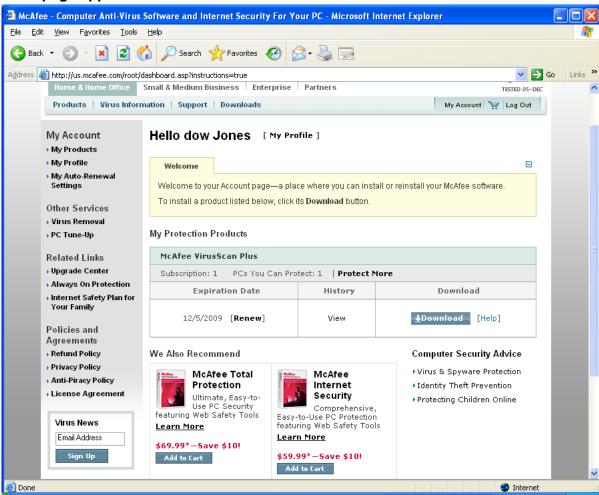
My Shopping Cart appears.

3. Leave Additional PCs drop-down at 0 (each additional will charge $10).
4. Enter the promotional code listed in the e-mail and click Submit Code.
   Refreshed shopping cart appears.
5. Click Checkout.
6. Enter information on next few pages to create a McAfee account and process the order. Then click Go to My Account.

Hello page appears.

7. Click the Download button in the middle of the page.
   Download process displays license agreement and several dialogue boxes to download and run/save application. Then the McAfee Security Center page appears.
8. *Leave the default installation option of Typical and click Next.*
   Status dialog appears for installing these applications: SecurityCenter, VirusScan, Personal Firewall, SiteAdvisor.

   Important: if you get an error message during the installation process, keep retrying until it works. If you chose to Run the file from the current location, you will have to download it again. If you chose to Save the file to your computer, you will have to launch the installation program again.

Installation Complete dialogue box appears explaining the important next step of clicking the icon in the taskbar.

9. Click on the McAfee icon in the task bar to start McAfee Security Center.
10. Click Fix.
11. Click the Scan button on the left side of the page.

Scan Options dialogue box appears.

12. Click Start for the **Full Scan.**
    McAfee scans computer, repairs as necessary, and displays the results of the scan.
13. Click OK.
14. Important: Reboot computer to finish the repairs.

Deluxe ID TheftBlock® Service Activation

The following information will help guide you through the registration process activating your protection using the Deluxe ID TheftBlock® services. We recommend that you compile all necessary information in advance and complete your registration within a single session:
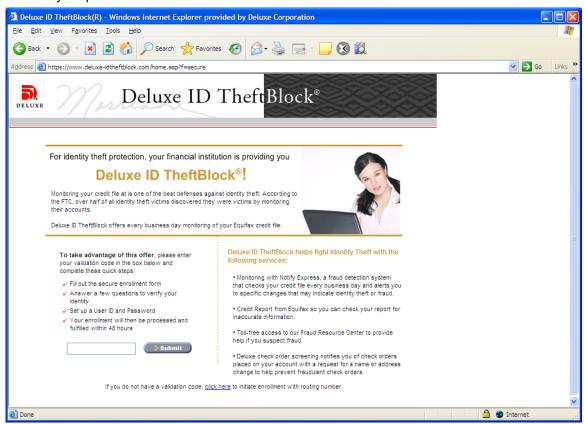
Validation code as provided in the e-mail.

Your name, social security number, date of birth, phone (home), e-mail, street address, city, state, and zip code.

Personal financial information appearing on your credit report such as loan pay-off amounts and monthly payments.

Instructions

1. Access the registration page by clicking this link.
https://www.deluxe-idtheftblock.com/secure

2. Enter your provided validation code in the box and click "Submit."

3. Enter your personal information into the registration screens and submit your order. You will then be provided with a confirmation message which completes your registration process.

At anytime if you need assistance you can call 1-800-839-9193 (option 6) to speak with a customer services representative. You can also access the FAQs at:
http://www.deluxe-idtheftblock.com/gs/english/Faq.asp

Frequently Asked Questions for Call Center Inquires

About the incident

1) Who is CheckFree?
CheckFree is a provider of financial electronic commerce services and products available through thousands of banks, billers and brokerage firms.

2) How could I have been redirected to a malicious site?
An unauthorized person used stolen credentials to log into CheckFree's account at its Internet domain registrar. We have subsequently created additional controls on that account so this kind of incident cannot happen again.

3) Who is responsible for this incident?
Federal law enforcement is continuing to investigate this matter. We cannot speculate about responsibility until the investigation is complete.

4) What does the (virus-Trojan-malware-malicious software) that was downloaded do?
The downloaded malicious software consisted of two programs that appear to perform a desirable function but in fact perform undisclosed malicious functions. We do know that the malicious software involved in this incident only affects computers equipped with the Windows operating system. Mac, Unix/Linux and other operating systems are not subject to either the initial or subsequent infection associated with this incident.

5) Has my data or information been stolen?
We are unaware of any fraudulent transfer of funds or theft of passwords, account numbers, or other confidential data associated with this incident. However, some but not all consumers who attempted to access our services between 12:30 a.m. and 10:10 a.m. EST on Tuesday, December 2, 2008 were misdirected to a server in Ukraine. This server displayed a blank page that was actually a PDF containing malicious software. If the consumer clicked on the page but had up-to-date virus protection, the malicious software download was thwarted and there were no adverse consequences. If the consumer's computer had no virus protection or its virus definition file was not current, the consumer may have downloaded malicious software.

6) Are my on-line banking and bill payment sites safe?
Yes, your on-line banking and bill payment site are safe. We have taken action with our domain name registrar that will absolutely prevent anyone from redirecting our sites in the future without our knowledge and consent.

7) How do I know that this won't happen again?
We have worked with the internet domain registrar to ensure that our sites cannot be redirected going forward without our specific knowledge and consent.

8) Which law enforcement agency is investigating this matter? Can you provide me with a case number or a contact person so I can track status myself?
The Federal Bureau of Investigation (FBI) has been the principal law enforcement agency leading the investigation since the incident occurred. However, they are not authorized to provide their investigative work product to the public at this time because that may compromise their ongoing efforts.

9) I am an online banking customer of (institution name) and I understand their customers were affected by this incident. I did not receive a notification letter and wonder why.
Notification letters were sent to all persons we believe may have been affected by the incident. Incorporate the questions. If you did not receive a letter but believe you were affected, we will send you instructions that will tell you how to detect and remove any malicious software from your computer and protect yourself against further risk.

About remediation steps

10) What should I do if I believe my identity has been stolen?
Both the Federal Trade Commission and the U.S. Department of Justice have excellent websites on this subject. We will send you instructions for accessing these sites.
- http://www.consumer.gov/idtheft (Federal Trade Commission)
- http://www.usdoj.gov/criminal/fraud/websites/idtheft.html (Dept. of Justice)

11) Why was I instructed to change my userid's and passwords? Have they been compromised?
It is simply good practice to take as many proactive steps as possible to prevent the possible breach of personal data. Changing your userid's and passwords will provide you with an additional level of protection. You should make it a practice to update your passwords periodically and to always use strong passwords, which contain a combination of letters and numbers.

12) Is the anti-virus software and identity protection really free?
Yes. There is no charge to you for the virus protection software and credit monitoring service we are providing to persons whose computers were infected with malicious software as a result of this incident.

13) I am having problems with the installation of the anti-virus software. What should I do?
We have included product support with McAfee as part of the free solution we are offering to customers. If you are having problems with the installation of the anti-virus software, please contact McAfee customer care at (866) 622-3911.

14) I am having problems with the anti-virus software you installed. What should I do?
We have has included product support with McAfee as part of the complimentary solution we are offering to customers. If you are having problems with the installation or operation of the anti-virus software, please contact McAfee customer care at (866) 622-3911.

15) I am having problems with the sign-up process for the (Deluxe ID Theft Block) credit monitoring service. What should I do?
We have has partnered with Deluxe ID TheftBlock. If you are having problems with the sign-up process, please contact them at (800) 839-9193.

16) Do I need to enroll in the credit monitoring service if I have contacted the credit bureaus and placed a fraud alert or credit freeze on my personal credit file?
They serve different purposes. For more information, please review the Federal Trade Commission or U.S. Department of Justice websites on this subject. We will send you instructions for accessing these sites.
- http://www.consumer.gov/idtheft (Federal Trade Commission)
- http://www.usdoj.gov/criminal/fraud/websites/idtheft.html (Dept. of Justice)

17) If my identity is stolen as a result of this incident, who is liable for my losses? What assistance will you provide?
If you take the precautions we have advised – checking your computer for the malicious software, keeping up-to-date virus protection in place, and enrolling in credit monitoring service – it is extremely unlikely that you will experience any negative consequences from this incident. However, once enrolled in Deluxe ID TheftBlock, you are eligible for assistance and reimbursement for covered losses – just in case.