



Fiserv, Inc.
4411 East Jones Bridge Road
Norcross, GA 30092

December 12, 2008

CONFIDENTIAL

Martha Coakley
Attorney General
State of Massachusetts
1 Ashburton Place
Boston, MA 02108-1698

Please be advised that CheckFree, a business unit of Fiserv, Inc., recently experienced an incident that may have resulted in the infection of certain consumers' personal computers with malicious software. Between the hours of 12:35 a.m. and 10:10 a.m. Eastern Standard Time on December 2, 2008, traffic to certain CheckFree-operated online bill payment websites was redirected without our knowledge or consent to a website based in Ukraine capable of infecting some but not all users' computers, depending on their computer's operating system and virus protection software.

This incident did not involve the compromise of the CheckFree online bill payment system or any CheckFree data at rest or in transit. To the best of our knowledge, there has been no unauthorized access to any information, including nonpublic personal information and sensitive customer information as those terms are defined by the Gramm Leach Bliley Act (GLBA) and GLBA regulations, and "personal information" as defined in the security breach notification laws of any state. However, the malicious software *could* have been used to download other software designed to transmit passwords, usernames and other information from the personal computer back to a server controlled by persons in Ukraine.

In response to this possibility, we and our client organizations are presently conducting a consumer notification. The notification describes the specific conditions under which the consumer would have been exposed (time of visit, computer operating system, virus protection status, visual description of the redirected site which looked nothing like the legitimate CheckFree sites) and directs potentially affected consumers to our call center for remedial actions. These actions include providing a McAfee software solution that will detect and remove the offending malicious software, as well as the provision of two years of credit monitoring service.

We estimate that approximately 160,000 consumers nationwide may have been exposed to the malicious software download attempt. However, it is not possible to determine which specific enrolled bill payment system users attempted to visit the CheckFree sites during the relevant time window on December 2, since those diverted never got there to log in. Thus, our notification program has been designed to reach and screen a much broader group of more than five million consumers, and 160,000 is an estimate of actual affected persons based upon typical traffic patterns. The McAfee and credit monitoring services capture zip codes of persons who respond to notification, which is happening mostly by email, and we can provide you with an estimate of your state's affected population when the remediation phase closes.

We have also notified the Federal Bureau of Investigation, the three major consumer reporting agencies, the five principal federal financial institution regulators, the Federal Trade Commission, the Securities & Exchange Commission, and the Commodities Futures Trading Commission. Certain information in this letter is not publicly known, and its disclosure could hinder the FBI investigation in progress, so Fiserv respectfully requests that the information contained in this letter be kept confidential. Should you have any questions regarding this matter, please contact me at 678-375-1265 or the address on this letterhead.

Sincerely,

James M. Jordan III, Esq.
Chief Privacy Officer
Fiserv, Inc.

APPENDIX A - CONSUMER NOTIFICATION

Letter to Bank Customers (institutions able to identify online users during incident window)

Date

<CUSTOMER NAME>

<ADDRESS>

<ADDRESS>

<CITY><STATE><ZIP>

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 and you should take the following actions:

- From the computer that was used to access online bill payment Tuesday, please go to (*link*) and follow onscreen instructions to scan your computer and remove any malicious software. This is a special utility developed by McAfee, the world's largest dedicated security technology company, to address this malicious software infection. You will need to enter validation code 000000 at the website to access this service.
- After you have removed any malicious software from your computer, please go to our online banking site (*link*) or contact (*number*) to reset your online banking ID/password. You may also wish to take this step for all other password-protected sites you access through this computer.
- You may also wish to accept our offer of a two-year subscription to Deluxe ID Theft Block Plus credit monitoring service so that you may monitor your credit report for unauthorized new accounts or changes to existing accounts. You may activate this service at (*link*) by entering validation code (00000000).

(Institution) values your business and your trust, and we apologize for any inconvenience this recent incident has caused. Please feel free to contact us at XXX-XXX-XXXX with any additional questions.

Thank you,

APPENDIX B - CONSUMER NOTIFICATION
Letter to Bank Customers (institutions unable to identify online users during incident window)

Date

<CUSTOMER NAME>
<ADDRESS>
<ADDRESS>
<CITY><STATE><ZIP>

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 them at (*number*) 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.

(Institution) values your business and your trust, and we apologize for any inconvenience this recent incident has caused. Please feel free to contact us at XXX-XXX-XXXX with any additional questions.

Thank you,

APPENDIX C - CONSUMER NOTIFICATION
Consumer-Facing Web Site Users – Content for In-Product & Email Notifications

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 at this site (*or site name, in email*) may be infected with malicious software that puts the security of your computer's contents at risk.

For a limited time period on Tuesday, December 2, 2008, some but not all visitors to this site (*or site name, in email*) were redirected from this 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 this service 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 within this site, 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 them at (*number*) 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. Please feel free to contact us at XXX-XXX-XXXX with any additional questions.

Thank you.