Standard Keylogging Notification Letter Format:

It has been brought to our attention by the United States Computer Emergency Readiness Team (US – CERT, http://www.us-cert.gov/) through the Multi-State Information Sharing and Analysis Center (MS-ISAC, http://www.msisac.org/) that a computer utilized around ***DATE TIME*** had been compromised with a software program that allowed capture of each keystroke. This computer was utilized to perform at least one transaction that contained information related to you.

US-CERT is a partnership between the Department of Homeland Security and the public and private sectors that monitors cyber space for threats and compromised information. If such information is located that involves citizens utilizing state or local government services, they inform the MS-ISAC which is a voluntary and collaborative organization with participation from all 50 states and the District of Columbia. MS-ISAC in turn notifies the applicable State's Chief Information Security Officer (CISO) so that the CISO can review the compromised information and take appropriate action. In the Commonwealth of Virginia, the Chief Information Security Office notifies the agency whose services were used by a citizen from a compromised machine so that notification to the citizen can be made.

Commonwealth of Virginia officials were informed that some of your information was found on a server located on the Internet. This computer which was used when you performed a ***TYPE OF TRANSACTION*** with the NAME OF AGENCY around ***TIMEFRAME*** was and still may be infected with malicious software, also known as malware. This malware could have been automatically installed on the computer without the user's knowledge in several different ways including:

- browsing to a web site and downloading infected programs
- opening an infected email
- allowing file-sharing on the computer
- outdated anti-virus software that did not identify and prevent the installation of the malware

This type of malware is generically referred to as a "key logger". Once installed on a computer, it records the information that anyone types and/or has stored on your computer (e.g. passwords and other personal information) and subsequently sends that data to the criminal(s) responsible for the installation.

The type of information that US-CERT found on the public server related to you included: ***LIST THE TYPE OF INFORMATION FOUND***. This may not be the only information that has been compromised. You should consider every use that was made of the infected computer as all keystrokes would have been logged and sent.

We are notifying you so that you can take any actions appropriate as you deem necessary. This compromise of your information is not a security problem caused by a Commonwealth system; however, we have an ethical obligation to inform you that your information was transmitted via the infected laptop or desktop computer system and may now be compromised.

Any computer you, or someone on your behalf, have used to access ***AGENCY WEBSITE*** around ***TIME*** is most likely compromised and should be cleaned and updated by a qualified technician.

If you own the computer utilized for this transaction, the malicious software should be removed from the computer as soon as possible. Once the malware is removed from the system, be sure to keep the anti-virus definitions up-to-date and scan your system for malware at least once a week. An excellent document on spyware can be found at http://www.us-cert.gov/reading_room/spyware.pdf. The following software can be used to detect and remove malware from your computer:

- Microsoft Windows Defender is a free program that helps to protect Windows-XP and Windows-Vista systems against pop-ups, slow performance and security threats caused by spyware and other potentially unwanted software. To find out more about Microsoft Windows Defender, please visit: http://www.microsoft.com/athome/security/spyware/software/default.mspx

- Spybot - Search & Destroy detects and removes spyware. Spybot-S&D is a free program that helps to protect Windows-2000, Windows-XP, and Windows-Vista systems against pop-ups, slow performance and security threats caused by spyware and other potentially unwanted software. To find out more about Spybot, please visit: http://www.safer-networking.org/en/spybotsd/index.html

To protect yourself, you may wish to place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. The credit reporting agencies used in the Unites States are:

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

For more information on identity theft, we suggest that you visit the Web site of the Federal Trade Commission at www.consumer.gov/idtheft.

If there is any further information we can provide you, please call ***XXX-XXX-XXXX*** to speak to ***Agency Information Technology Security Director, give name***.

Sincerely,