

Responses to Frequently Asked Questions

What happened?

An Agency of Human Services (AHS) computer, not website, that housed information related to the federally mandated Office of Child Support (OCS) bank match application – including names, social security numbers and bank account data – was removed from service last month when we discovered that the computer had a virus. Agency staff was cleaning the computer after a virus attack when they discovered suspicious activity.

Initial forensic examinations by AHS CIO staff, with participation from the Vermont Internet Crimes Task Force, indicated that it was an automated attack and not a targeted attack by an individual. The computer had several vulnerabilities that had been exploited to install malicious software, in an attempt to utilize the resources of the computer for video-relay and other purposes. From AHS' initial examinations there was no evidence to indicate that any personally identifiable or financial information was obtained by unauthorized users.

However, because of our sensitivity to privacy concerns, AHS contracted with Bearhill Security - an information security consulting firm – to complete a thorough, external, forensic review. We just received the results of this complete forensic review and while there is still no evidence that confidential files were accessed, unfortunately, there is also no evidence that they were not accessed.

How is the State responding?

AHS is taking steps to notify all affected individuals and provide suggestions regarding how to protect themselves to avoid or reduce any potential harm that might come from misuse of personal information. These suggestions include requesting credit reports and monitoring bank statements. AHS will be sending out notification letters January 30 and 31 to all affected individuals; included in the letters will be information regarding a premier credit monitoring service the state is offering for free. This service will notify individuals of any suspicious activity on their credit reports. We have also established a toll-free number – 1-888-832-1488 – which customers can call if they have any specific questions.

Over the last several days we have been communicating with the affected banks and credit unions to inform them of the situation. None of the banks or credit unions have reported any unusual activity on their accounts. We have worked with

the Vermont Internet Crimes Task Force, contacted the Vermont State Police and met with the FBI, the Attorney General's office and the Department of Banking, Insurance, Securities and Health Care Administration (BISHCA).

Over the past year the state has been aggressively strengthening its information security practices on a number of levels. The state hired a Security Director, as did AHS. We have been updating policies, auditing systems and taking action to increase security. It is important to note, however, that this computer was a unique single purpose application not the state's larger computer system. The state's internal network is very secure.

Why was my information on this computer?

Federal and state law mandates that states use certain enforcement tools to collect delinquent child support payments. One of these tools used by OCS is an application that runs a quarterly match with nine Vermont banks and credit unions to establish whether delinquent non-custodial parents have assets that can be frozen and used to reduce the support owed.

OCS provides an encrypted list of names of non-custodial parents (including social security numbers and dates-of-birth) who are three months or more in arrears on child support payments, to the nine participating financial institutions. The banks and credit unions, in turn, match the names against their list of customers. If any matches are found, information including account numbers, account balances and names of any joint account holders in encrypted format is returned to OCS.

The computer had a firewall and the data transmissions were encrypted, however during the forensic investigation we discovered that the firewall was inadequate and the data was retained on the computer, sometimes in an unencrypted format, after the OCS match was made. The original system design called for retaining the data on the computer. This practice has ended and going forward will not be acceptable for any AHS application.

How do I know if my information is at risk?

All affected individuals will be receiving letters in the near future – if you do not receive a letter, your personally identifiable information was not on the OCS computer.

Three sets of individuals' data were stored on the compromised computer:

- 1) List of names of non-custodial parents (including social security numbers and dates-of-birth) who were three months or more in arrears on child support payments, provided by OCS to banks – approximately 8,300 individuals;
- 2) List of names and bank or credit union account information for persons who were behind on their child support payments and any joint account holder information, provided by 9 financial institutions to OCS – approximately 2,800 individuals. The 9 affected banks and credits unions are CVPS Employees Credit Union; First Brandon National Bank; Federal Family Credit Union; Granite Hills Credit Union; Merchants Bank; New England Federal Credit Union; Northfield Savings Bank; Opportunities Credit Union; and VT State Employees Credit Union;
- 3) List of names and account information, which was part of a larger encrypted data file sent to AHS by New England Federal Credit Union (NEFCU). On two occasions, one in July of 2004 and another in October of 2005, NEFCU chose an option of communicating encrypted data files to the state, by following an approved method outlined in federal guidelines, but not the one used in Vermont. This resulted in the transmission of a larger than required file of account information. The State processed this transmission and extracted the information required for OCS enforcement. This larger file of account information was retained on the OCS computer through the time of the compromise and contains the information of approximately 58,800 individuals.

Why were there only nine banks affected?

All financial institutions are required by federal law to participate in data match efforts to recover delinquent child support payments. Other, often larger, Vermont banks/credit unions transmit required information through a different method, operated by the federal government. This method was not affected by the recent computer security incident.

Is the reason for the security compromise the fact that a particular Microsoft Patch was not loaded?

We know now that the system had several weaknesses that could have been exploited, including the fact that a particular Microsoft security patch was not installed in a timely manner. Unfortunately, we have no way to determine what particular weakness was exploited. As stated earlier, we have already taken steps and will continue with efforts to strengthen our information security practices on a

number of levels, to ensure that such a compromise does not occur again in the future. It is important to note that by definition Microsoft patches are generally released after a vulnerability has been discovered and in this case there is evidence of suspicious activity that occurred on the computer prior to this particular patch being released.

You have stated that it was an automated attack but press articles quote the Forensics Report as saying "the server was under the control of a person." Why the discrepancy?

Based on the evidence in the Forensics Report, we believe the nature of this particular incident was an automated attack, where malicious software was remotely installed on the computer allowing it to become part of a "botnet." Botnet is a term for a collection of compromised machines – often hundreds – running programs autonomously, usually "worms," "Trojan horses" or "backdoors," under a common command and control infrastructure. Obviously there is an individual that launches these larger scale attacks but that individual controls the botnet remotely, often in an attempt to launch "denial of service attacks" or to relay items like pirated movies and television shows. For example, during the forensic analysis we discovered an episode of a current television program on the computer.

Regardless of the nature of the attack, and while there is still no evidence that confidential files were accessed, unfortunately, there is also no evidence that they were not accessed. AHS is taking proactive steps to notify all affected individuals and provide suggestions regarding how to protect themselves to avoid or reduce any potential harm that might come from misuse of personal information.

Press articles also quote a Norwich University Professor saying the system had "limited security protection" and a design that hadn't been used in "more than 10 years" – is that the case?

Prior to 2004, single purpose systems that interfaced with external entities like banks, were generally not built on the state's more secure internal network (GOVNET) in order to protect the state's internal databases. This particular single purpose system did have a firewall but it did not provide the necessary protections. Today with more advanced security measures we build these types of applications within our internal network, with enhanced security that prohibits these external parties from access to other state systems. As stated earlier, we have already taken steps and will continue with efforts to strengthen our information security practices

on a number of levels, to ensure that such a compromise does not occur again in the future.