



## Human Services Department Frequently Asked Questions Information Technology Breach

### 1. **Question: What is an Information Technology (IT) breach?**

**Answer:** An information technology breach is when one or more persons gains unauthorized access to an electronic data system. In this case, the security breach involved unauthorized access to personal information through the Human Services Department's (HSD's) child support enforcement website (eCSES).

### 1. **Question: When was the IT breach within the HSD website discovered?**

**Answer:** HSD identified and stopped unauthorized access to the department's eCSES website on July 13, 2008.

### 2. **Question: How was the IT breach discovered?**

**Answer:** The department's new Chief Information Officer (CIO) - a fresh set of eyes - recognized some irregularities in the eCSES system and requested an internal audit be conducted. HSD's internal audit bureau chief in the Office of Inspector General confirmed the irregularities as an IT breach. The department immediately stopped the breach and began the full investigation.

### 3. **Question: Why did the IT breach happen?**

**Answer:** HSD has determined with the help of external contractors that its IT system was not configured as securely as it could have been. Since the breach occurred, the department has completely shut down the eCSES system, contracted with nationally recognized security firms, and rebuilt the system with the best security configurations possible.

### 4. **Question: During what period of time was personal information at risk due to the breach?**

**Answer:** The website was accessed by multiple internet hackers at various times between September 9, 2006 and July 13, 2008.

### 5. **Question: Was information taken during the IT breach?**

**Answer:** Yes.

### 6. **Question: What kind of information was taken?**

**Answer:** Personal information of child support custodial parents, non-custodial parents, children, employers who withhold wages for non-custodial parents and possibly HSD employee information was accessed during the IT breach. Personal information includes names, dates of birth, social security numbers, and bank information.

### 7. **Question: What IT systems are affected by the breach?**

**Answer:** The department has three major systems, CSES (for Child Support Enforcement), MMIS (for Medicaid claims), and ISD2 (for program eligibility). In addition HSD operates the eCSES



## Human Services Department Frequently Asked Questions Information Technology Breach

website and a Data Exchange Server, which moves information back and forth through all of the systems. It was eCSES and the Data Exchange Server that were compromised by the IT breach. Data in the Child Support Enforcement System prior to July 13, 2008 is at risk from the breach. Data in the ISD2 and MMIS systems, between the dates of September 9, 2006 and July 13, 2008 is also at risk due to the breach. Some personal information about HSD employees is also possibly at risk, but it is not definitive if this information was compromised. Medicaid provider information and Medicaid clients' personal health information was not compromised by the breach.

**8. Question: When will HSD know for sure if personal information was indeed stolen?**

**Answer:** Because of the sophistication of the hackers, we may never know for sure the extent of the information taken.

**9. Question: Are there people outside of New Mexico affected by the breach?**

**Answer:** Yes. HSD serves clients – custodial and non-custodial parents and children – and interacts with employers both inside and outside of New Mexico that may be affected by the breach.

**10. Question: How is the Human Services Department planning to notify people of the IT breach?**

**Answer:** HSD is issuing Public Service Announcements on radio stations across the state as well as print public notices in newspapers across the state and nationally alerting people of the problem.

**11. Question: What is HSD doing to assist persons whose information may have been compromised due to the breach?**

**Answer:** HSD is encouraging its clients, customers, custodial parents, non-custodial parents, employers, and department employees who may have been affected by the IT breach to have a 90-day fraud alert placed on their credit bureau file, free of charge. Fraud alerts tell creditors to contact the individual before any new accounts are opened or existing accounts are changed. Individuals may contact any one of the three major credit bureaus to request a fraud alert, and may request such an alert be extended every 90 days. The one credit bureau notified will notify the other two, which then also must place fraud alerts in that person's file.

- Equifax – 1-800-685-1111, [www.equifax.com](http://www.equifax.com)
- Experian – 1-888-397-3742, [www.experian.com](http://www.experian.com)
- TransUnionCorp – 1-800-680-7289, [www.transunion.com](http://www.transunion.com)

HSD has also set up a webpage on its general website ([www.hsd.state.nm.us](http://www.hsd.state.nm.us)) where people can access the credit bureaus above as well as a link to the New Mexico Attorney General's Identity Theft Prevention and Repair Kit. The department has also set up a toll-free call center for people who do not have access to the internet and need assistance in contacting a credit bureau. The call center will



**Human Services Department  
Frequently Asked Questions  
Information Technology Breach**

be available 9:00 a.m. to 5:00 p.m. (MST), Monday through Friday beginning November 24, 2008. The call center numbers are: In State – 1-877-719-3337 and Out of State – 1-877-719-3338.

**12. Question: If HSD knew about the IT breach in July, 2008, why is it just now releasing a notification?**

**Answer:** While the department knew about the IT breach in July, 2008 the department did not know the extent of the breach at that time. A forensic investigation looked over millions of lines of logs of information to determine the extent of the breach, which took months to complete.

**13. Question: Does New Mexico have laws requiring notification regarding computer security breaches?**

**Answer:** No. However, New Mexico is doing exactly what other state's laws require for those states that have statutes on this issue.

**14. Question: What steps has HSD taken to repair the IT breach?**

**Answer:** HSD stopped, investigated and has now rebuilt the entire eCSES system and Data Exchange Server. HSD is also implementing new policies and processes for changes to assure this will not happen again.

**15. Question: Is personal information in the HSD systems safe now?**

**Answer:** Yes. HSD worked quickly to secure the department's websites and data and is confident the IT systems are at the safest levels ever.

**16. Question: Are IT systems of other state departments safe?**

**Answer:** DoIT is working with HSD and other state departments to evaluate their IT security systems to ensure they are operating at the highest and safest levels. The state has made significant improvements to its systems to protect confidential information. DoIT staff is on constant alert to ensure state data is as safe as possible.

**17. Question: How often do Internet hackings occur?**

**Answer:** Internet hacking is constantly occurring. State, federal and private business systems are under regular attack, so IT security requires vigilance to identify and address IT breaches and increase security as HSD did in this case.

**22. Question: Are there other examples of recent IT security breaches?**

**Answer:** Yes.

- 1) The City of San Francisco
- 2) TJ MAX
- 3) Veterans Administration