

# Situation Briefing - ODOC Information Security Breach

February 9, 2011

- On Thursday, Jan. 27, 2011, DOC officials received word that there had been a potential information security breach, when a non-employee member of the general public reported being in possession of a portable digital storage device that contained DOC payroll reports from Warner Creek Correctional Facility, Deer Ridge Correctional Institution and Shutter Creek Correctional Institution.
- The department immediately began an investigation to verify the report, and to determine what data may have been included on the portable digital storage device in question. The Oregon State Police were notified and are conducting their own investigation, and are assisting DOC with its internal investigation. We are unable to disclose the particulars of how the payroll information got into the hands of the public at this time because the investigations are ongoing.
- Because the portable digital storage device was damaged prior to the department receiving it, we cannot know with complete certainty what was on it. Initial forensic findings indicate that at least two types of information may have been breached:
  - **Staff members' personal information, including SSNs\* (Group 1)**
    - Payroll reports from Warner Creek Correctional Facility (WCCF) from July 31, 2005 to Sept. 30, 2007, which included names, social security numbers and other payroll information similar to what's found on a pay stub.
    - Payroll reports from Deer Ridge Correctional Institution (DRCI) from Aug. 31, 2006 to Sept. 30, 2007, which included names, social security numbers and other payroll information similar to what's found on a pay stub
  - **Staff members' personal information, not including SSNs (Group 2)**
    - Payroll reports from Warner Creek Correctional Facility, Deer Ridge Correctional Institution and Shutter Creek Correctional Institution (SCCI) from Oct. 1, 2007 to present, which included staff names and other payroll related information similar to what's found on a pay stub. These reports did **not** include social security numbers.
- The scope of the breach is just under 550 total staff members. DOC employs approximately 4,500 employees across the state of Oregon.

\* Personal information is defined by ORS 646A.602(11)(a) to (c).

- The investigation has thus far been unable to determine if data from the portable digital storage device was at any point transferred to computers outside of the department's control.
- We do not believe that the breach was malicious.
- We do not have reason to believe staff at institutions other than WCCF, DRCI or SCCF should be concerned at this time.

## **Group 1**

- As a precaution, DOC has contracted with ID Experts®, a data breach and recovery services expert out of Portland, Ore.
- ID Experts will provide staff, whose personal information (names and SS#s) was potentially breached, with fully managed recovery services including:
  - 12 months of credit and CyberScan monitoring
  - A \$20,000 insurance reimbursement policy
  - Educational materials; and
  - Access to fraud resolution representatives
- This service is being offered to affected staff members (those whose names and social security numbers were breached) free-of-charge. The Department is paying for the service as a part of its contract with ID Experts, and is recommending affected staff take advantage of the offer.
- Affected staff members will be mailed a notification letter directly from ID Experts, Thursday, Feb. 10, indicating that they were a part of the personal information breach and explaining how to opt-in to the credit monitoring service.
- The nature of the breach enabled DOC to identify all individuals who are eligible to receive services from ID Experts.
- ID Experts representatives will be available via call center, beginning Friday, Feb. 11, to assist staff with questions, concerns and enrollment into identify protection services.
- Call center hours are Monday through Friday, 6 a.m. to 6 p.m. PST. The call-in number is 1.877.819.8682. Callers must have an access code, included in their individual notification letters, to access services.
- The call center will be online from Feb. 11 to May 11, 2011.
- Contract cost to DOC:

\* Personal information is defined by ORS 646A.602(11)(a) to (c).

## Group 2

- DOC will also send internal notification to the second group of staff members, indicating that WCCF, DRCI and SCCF staff members' payroll information from Oct. 1, 2007 to present (which is normally exempt from release to the public) was also on the portable digital storage device.
- For this group, however, ***no employee SSNs or other personal information that could be used by third parties to engage in identity theft was disclosed.***
- As such, the department will not be offering ID theft protection services, including credit monitoring services, to this group of employees.

## Site Visits

- DOC officials will be conducting site visits at WCCF, DRCI and SCCI to answer questions, and talk with concerned employees. The visits are scheduled between Feb. 16 and 18, 2011, with specific information to come later.

## Other Important Information

- As of Oct. 1, 2007, state law prohibited the printing, displaying or posting of social security numbers in documents, reports, materials, other records, etc...unless redacted first. As of Oct. 1, 2007, new documents, reports, materials, other records, etc... essentially could not be produced with SS#s on them.
- In addition to notifying staff of the breach and providing credit monitoring services to Group 1, DOC is continuing to investigate the situation to determine exactly how the portable digital storage device got into the hands of a non-employee, member of the public.
- DOC is also examining internal practices to seek to ensure that the security of personal information is never again breached, to the degree the department can impose policies, procedures and controls over use, storage and transportation of employee personal information from one location to another.
- DOC will update staff internally, when results of its internal review are finalized.