

HUD inadvertently exposed personal information of nearly 500,000 individuals

Social security numbers, dates of birth posted on public website

November 21, 2016

[Ben Lane](#)

[2 Comments](#)

KEYWORDS [data breach](#) [Department of Housing and Urban Development](#) [HUD](#) [Identity theft](#) [Public housing](#) [public housing agencies](#)



Nearly 500,000 individuals are at risk of identity theft after the **Department of Housing and Urban Development** inadvertently made their personal information — including social security numbers and dates of birth — publicly available on its website.

According to HUD, the data breach is the result of two separate incidents, one of which exposed the personal information of more than 425,000 public housing residents.

In an announcement posted to HUD's website, Helen Goff Foster, HUD's executive secretary and senior agency official for privacy, said that the agency discovered the breaches recently and removed the individuals' personal information, but is currently unable to determine how many people accessed the sensitive information.

The larger of the two breaches involves the personal information of public housing residents.

HUD said it discovered this breach on September 14. Prior to discovering the breach, the personal information of 428,828 public housing residents may have been publicly available.

"While sharing community service requirement information with local public housing authorities, HUD discovered that personal information was made available through its website," HUD posted on its website.

Under that requirement, public housing residents between the ages of 18 and 62 are required to perform 8 hours of community service each month, unless otherwise excused for work or education conflicts.

But instead of sharing that information privately with the housing authorities, Excel files with 428,828 individuals' personal information was made publicly available on HUD's website.

According to HUD, the file included the public housing residents' last name, last four digits of their social security number, and their building code identifiers.

HUD said that it made these postings five separate times beginning in August 2015, but removed the information from its website on Sept. 22, 2016.

Additionally, HUD said that the name, full or partial social security number, and address of an additional 50,727 individuals was exposed in a separate breach.

That breach involves individuals who live in areas designated as part of HUD's Empowerment Zone, Enterprise Community, and Renewal Community Initiatives, which are efforts that seek to reduce unemployment and generate economic growth through the designation of federal tax incentives and award of grants to distressed communities.

Employers that hire EZ, EC and RC residents are eligible for tax incentives. As part of this effort, HUD developed an "EZ/RC Locator," which helps employers determine whether employees' addresses were in the designated geographic areas.

But until Aug. 29, 2016, the personal information of 50,727 individuals was inadvertently made available on HUD's website in an Excel file and searchable via Google, HUD

said.

According to HUD, this breach exposed the name, full or partial social security numbers, and address, and in some cases, the date of birth, income, and demographic information of 50,727 individuals.

HUD said that a review revealed that, despite the EZ/RC locator instructions requesting that only addresses should be uploaded into the system, approximately 20% of third-party employers and tax preparers using the Locator uploaded spreadsheets containing unnecessary personal information, including names, social security numbers, and date of birth.

HUD noted that it did not request and does not need this “extraneous” information, and HUD was not aware that the information was “erroneously uploaded” to its website until it was reported in late August.

Upon discovering the breach, HUD made the information private.

HUD said that it conducted further review to determine the scope of these incidents, the extent of data exposed, and likelihood of unauthorized use of the information.

“To date, HUD has no evidence that any of the data has been used inappropriately,” HUD said.

As a result of the breaches, HUD is sending letters to the affected individuals and offering them one year of credit monitoring services from **TransUnion**.

The letter, signed by Goff Foster, states that HUD does not know if the individual’s information was accessed or used during the time it was available on HUD’s website.

“HUD deeply regrets this error,” the letter reads.

“HUD is committed to protecting the personal information with which we are entrusted,” Goff Foster’s letter continues. “We are continuing to take steps to proactively identify and address security risks to our systems and information. On behalf of the Department, I sincerely apologize for any inconvenience this incident may cause you.”

[Reprints](#)

Related Articles

[HUD watchdog warns of scammers offering phony housing grants](#)

[HUD proposes new rule to further protect victims of harassment](#)

[HUD: Children still overexposed to lead paint dangers](#)



Ben Lane is the Senior Financial Reporter for HousingWire. In this role, he helps set a leading pace for news coverage spanning the issues driving the U.S. housing economy. Previously, he worked for TownSquareBuzz, a hyper-local news service. He is a graduate of University of North Texas. Follow Ben on Twitter at @BenLaneHW.

Recent Articles by [Ben Lane](#)

[CoreLogic chooses Frank Martell to replace Anand Nallathambi as president, CEO](#)

[Flagstar closes acquisition of Stearns Lending delegated correspondent lending business](#)

[CoreLogic President and CEO Anand Nallathambi passes away](#)

[Ben Carson sworn in, spends first day as HUD Secretary](#)