Survivor Privacy Incident

Release Date: Sep 13, 2019

In March 2019, the U.S. Department of Homeland Security Office of the Inspector General (DHS OIG) reported that the Federal Emergency Management Agency had unnecessarily overshared sensitive, personally identifiable information of some disaster survivors with its contractor that supports its Transitional Sheltering Assistance (TSA) program. In response to this incident, FEMA acted quickly to ensure that overshared information was quarantined, protected, and permanently removed from the contractor's system.

While we regret this error, the Agency will continue to assure disaster survivors that it has not found any evidence that any of the overshared information was compromised. Out of an abundance of caution, FEMA will provide credit monitoring services for a period of 18 months to affected survivors who request the service. Instructions to contact FEMA, request free credit reporting, or register for free credit monitoring will be identified in a FEMA notification letter sent today to affected disaster survivors.

FEMA apologizes for any concern this overshare may have caused for disaster survivors; it remains committed to protecting and strengthening the security of disaster programs to help people before, during, and after disasters.

FEMA remains committed to protecting and strengthening the integrity, effectiveness, and security of our disaster programs that help people before, during, and after disasters.

- Letter to survivors
- Frequently asked questions

Letter To Disaster Survivors

On September 3, 2019, FEMA notified disaster survivors of the privacy incident and sent the following letter with instructions to contact FEMA, request free credit reporting, or register for free credit monitoring on their own.

Dear Survivor,

I am writing to inform you of a privacy incident involving the Federal Emergency Management Agency's (FEMA) overshare of disaster survivor information with a contractor that supports FEMA's Transitional Sheltering Assistance (TSA) program. You are receiving this notification because you are listed as someone who was affected by a Presidentially-declared disaster and were eligible for assistance through this program. We have determined that your personal information was impacted by this privacy incident.

The TSA program provides hotel accommodations for disaster survivors who are not able to return home for an extended period following a disaster. FEMA relies on contractor assistance to administer the program, which involves payment directly to lodging providers. A version of FEMA assistance necessitated sharing banking and address information with the contractor to reimburse disaster survivors directly for hotel and lodging costs, rather than paying lodging providers directly. As FEMA has not activated that program since 2008, the sharing of survivor banking and home address information with the contractor ceased to be necessary. However, FEMA continued to share the same level of information previously required. This resulted in an oversharing of survivor information.

What happened?

During the course of an ongoing audit of FEMA's TSA program conducted by the Department of Homeland Security's (DHS) Office of Inspector General (OIG), it was discovered that FEMA shared more than the required personally identifiable information (PII) of disaster survivors, to include sensitive PII (SPII), with a FEMA contractor. This overshared SPII included disaster survivors' banking and home address information.

What information was compromised?

The overshared data included survivor banking and address information, which was no longer necessary because FEMA provided payments directly to hotels through the contractor, instead of reimbursement to survivors. FEMA conducted its own extensive review of the incident and determined that it overshared the address information of 2.5 million individuals with the contractor. Additionally, of the total 2.5 million impacted individuals, approximately 1.8 million individuals also had their banking information overshared with the contractor. FEMA believes any Individual Assistance (IA) applicant who shared their address and banking information at the time they registered for FEMA assistance since 2008, and were eligible for TSA, may have had their information transferred to the contractor.

What has/is FEMA doing to rectify this incident?

FEMA takes personal privacy very seriously. We are working to protect the information of disaster survivors and prevent similar incidents from occurring in the future. Notification letters are being sent to those who were affected by the overshare of SPII. All individuals affected by this privacy incident are being offered 18 months of free credit monitoring and identity protection services. FEMA also established a webpage at www.fema.gov/survivor-privacy-incident to provide notice to individuals along with remediation options. In addition, FEMA took the following actions after identifying this error:

- Permanently deleted previously-overshared PII and SPII from the contractor's computer system.
- Immediately changed our data-sharing process and only share the minimum amount of data necessary for our contractor to run the TSA program.
- Conducted a security assessment of the contractor computer system and determined there was no evidence that disaster survivor information had been compromised.

What do I need to do?

FEMA has not found any evidence that your overshared PII or SPII was compromised. However, in order to minimize any potential risk, FEMA has arranged to have MyIDCare provide credit monitoring services to protect your identity for eighteen (18) months at no cost to you. You may sign up via phone at 1-833-300-6934 or online at the following web page, using the redemption code at the upper right-hand corner of the first page of this letter: https://ide.myidcare.com/emergencylodgingIPS

You can also visit www.fema.gov/survivor-privacy-incident or speak directly with an individual about this matter by calling 1-833-300-6934, Monday through Saturday, 9:00 a.m. through 9:00 p.m., Eastern Standard Time (EST). We will be able to answer your questions about what happened and provide you with information on how you can monitor the security of your personal information.

What else can you do to protect yourself?

You may obtain a free credit report by contacting AnnualCreditReport.com or by calling 1-877-322-8228. You may also contact the three major credit bureaus below regarding credit freezes and credit reports:

Experian.com
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

Equifax.com
P.O. Box 105069
Atlanta, GA 30348-5069
1-800-525-6285

TransUnion.com
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

Review your free credit report carefully. If you find errors, take these steps:

- Explore if a credit freeze is right for you. You have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent anyone from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. By law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies.
- You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies. The agency you contact will then contact the other two credit agencies.
- Dispute any errors you find yourself. You don't need to use a credit repair service. By law, consumer reporting agencies and the creditors that provide the information in your credit report are responsible for correcting inaccurate or incomplete information in your report.
- If errors on your credit report seem to be the result of someone stealing your identity, go to identitytheft.gov to get personalized steps to report and recover from identity theft.

FEMA takes very seriously the obligation to serve disaster survivors and is committed to protecting the information entrusted to us. We sincerely apologize for any inconvenience this may have caused. Please be assured that we will make every effort to ensure this does

not happen again in the future. Our goal remains protecting and strengthening the integrity, effectiveness, and security of our programs that help people before, during, and after disasters.

Frequently Asked Questions

Why did I receive a letter from FEMA about a privacy incident?

Sometime between 2008 and late 2018, you applied for disaster assistance and were eligible to receive emergency lodging through the Transitional Sheltering Assistance, or TSA, program. Disaster survivors who were determined eligible for the TSA program had their information overshared with the contractor responsible for executing the TSA Program. FEMA, in coordination with the DHS Office of Inspector General, identified that the incident involved the oversharing of sensitive, personally identifiable information of disaster survivors. As part of the remediation strategy, FEMA is notifying impacted disaster survivors through this letter and providing credit monitoring services to those impacted by this overshare.

If you would like, you can go to https://ide.myidcare.com/emergencylodgingIPS to sign up for free credit monitoring and identity protection services.

How do privacy incidents occur?

A privacy incident happens when sensitive data (like bank account information) is compromised, which means it has the potential to be seen, stolen or used by an unauthorized individual. Here, the incident occurred because FEMA overshared your information with an authorized FEMA contractor.

A more formal definition of a privacy incident is that it is, “the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, have access or potential access to PII in usable form, whether physical or electronic, or where authorized users access PII for an unauthorized purpose.

What information was compromised?

The overshared data included survivor banking and address information. FEMA conducted its own extensive review of the incident and determined that it overshared the address information of 2.5 million impacted individuals, of which approximately 1.8 million individuals also had their banking information overshared with the contractor.

Why/how did this happen?

FEMA overshared disaster survivor information with one of its contractors because the agency did not update its data transfer process after making a change in the operation of the Transitional Sheltering Assistance program. FEMA relies on contractor assistance to implement TSA, which provides hotel accommodations for disaster survivors unable to return home for an extended period following a disaster.

At one time FEMA administered the TSA program as a reimbursable program, for which FEMA's contractor needed banking and address information to reimburse disaster survivors directly for lodging costs. However, after 2008, the sharing of survivor banking and home address information with the contractor was unnecessary. FEMA continued to share the same level of information previously required. This resulted in an oversharing of survivor information.

Is my information still at risk?

Based on our security assessment, FEMA found no evidence information overshared with the contractor was compromised, and we believe it's unlikely your information previously overshared is currently at risk. FEMA also worked with the contractor to permanently remove all of the overshared information from their system. However, we recommend considering safeguarding your identity and taking advantage of available resources out of an abundance of caution.

Was my information hacked?

No. FEMA has not found any evidence that your personally identifiable information has been compromised by unauthorized users while in the possession of our contractor.

How many people were impacted by the incident?

Approximately 2.5 million disaster survivors were impacted by the incident. Those who were impacted were sent a notification letter via U.S. Mail.

What has FEMA done to resolve this incident?

After identifying the oversharing error, FEMA took the following actions:

- Permanently removed all overshared Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII) from the contractor's computer system.
- Immediately changed our data-sharing process and only share the minimum amount of data necessary for our contractor to run the TSA program.
- Conducted a security assessment of the contractor computer system and determined there was no evidence that disaster survivor information had been compromised.

I received a letter from FEMA stating that my information was overshared with a FEMA contractor. However I never applied for disaster assistance myself. Why was I contacted by FEMA?

In 2017, FEMA identified situations where FEMA disaster assistance applications were submitted using someone else's personal information. In response, FEMA notified survivors by phone or email at that time that their information may have been used to create a potentially fraudulent registration for FEMA assistance.

You received as a letter from FEMA this month because our records indicated that your personal information was overshared with FEMA's contractor. Whether the information was provided to FEMA by you or by a fraudulent party, we encourage you to protect yourself by taking advantage of the credit monitoring services offered at no additional cost to you.

The letter I received from FEMA this month said I applied for assistance sometime between 2008-2018. Why is FEMA only notifying me just now?

Once FEMA became aware of the data oversharing, the agency worked rapidly to ensure the contractor's data system was secure and all unnecessary data was permanently removed. The notification process underway now was initiated as soon as FEMA was able to confirm which survivors needed to be notified, and FEMA was able to put adequate services and support in place for those affected

survivors.

I received a call from FEMA about free credit monitoring services. How do I know this is not a scam?

You will not receive an unsolicited phone call from FEMA or the identity protection and credit monitoring service providers. We will not reach out to you regarding this incident unless you specifically ask to have someone from FEMA to call you to discuss this issue. If you are contacted by anyone asking for your personal information in relation to this incident, do not provide it.

If I sign up for these services, will it cost me anything?

No. FEMA is offering these services for 18 months free of charge. Your membership will end after 18 months. You can decide to re-enroll on your own if you would like to have these services beyond 18 months.

I received hotel assistance when I had to evacuate my home during a disaster, but I did not receive a letter from FEMA. Can I get this free service?

FEMA began sending the notification letters on September 3, 2019. If it has been more than 2 weeks, and you believe you should have received this letter, please call the FEMA Emergency Lodging ID Services Helpline at 1-833-300-6934.

Why have deceased individuals been notified?

Please accept our deepest sympathies on the loss of your loved one. A deceased individual may have been sent a notification letter because we determined his/her information was included in the TSA Data Overshare. Our goal is to provide the information and tools to protect the deceased individual's identity and credit.

We are providing a comprehensive suite of credit monitoring services. Each year, thieves steal the identities of nearly 2.5 million deceased Americans. To reduce the likelihood of any misuse, we are offering credit monitoring services for deceased individuals who were impacted. How can I further protect my deceased loved one's identity?

Below are a few tips to reduce the risk of having a deceased person's identity stolen:

- Send the IRS a copy of the death certificate, which is used to flag the account to reflect that the person is deceased.
- Send copies of the death certificate to each credit reporting bureau asking them to put a "deceased alert" on the deceased's credit report

Which/what type of disaster survivors who used the TSA Program were impacted?

FEMA believes anyone who registered for disaster assistance since 2008 and was eligible for Transitional Sheltering Assistance, may have been impacted.

What states and territories did the TSA program operate in?

TSA has been activated in the following 12 states and territories over the previous 11 years:

1. California
2. Colorado
3. Commonwealth of the Northern Mariana Islands (CNMI)
4. Florida
5. Louisiana
6. New Jersey
7. New York
8. North Carolina
9. North Dakota
10. Pennsylvania
11. Puerto Rico
12. Texas