CATHOLIC COMMUNITY SERVICES AND CATHOLIC HOUSING SERVICES
AUTOMATIC FUNDS TRANSFER SERVICES, INC. DATA INCIDENT FAQS

Q. What happened?

A. On February 5, 2021, our third-party check processor, Automatic Funds Transfer Services, Inc. (AFTS), notified CCS/CHS that its servers were encrypted by ransomware. AFTS has advised CCS/CHS that it engaged outside forensic consultants to determine what information may have been involved in the incident. While AFTS's investigation is ongoing and may evolve, we understand from AFTS that the incident does not appear to affect any information that AFTS stores for CCS/CHS. CCS/CHS's activities with AFTS have ceased and paper check transactions are being processed directly by CCS/CHS.

Q. When did this happen, and when did you learn about it?

A. According to AFTS, the incident occurred on February 3, 2021. AFTS notified us on February 5, 2021. Upon learning of the incident, we immediately began investigating to determine what information about our donors may have been involved. Although AFTS's investigation is ongoing and may evolve, we understand from AFTS that it does not appear that CCS/CHS donor information was involved in the incident. We nevertheless opted to voluntarily notify our donors as soon as possible out of an abundance of caution and in the spirit of full transparency.

Q. What are you going to do to prevent this from happening again? What security protections have you put in place to better protect information following this incident?

A. The safety and protection of our donors' information is our highest priority and we recommend that donors monitor their bank/checking accounts for signs of unusual activity. Although we understand from AFTS that it does not appear that CCS/CHS donor information was involved in the incident, paper check transactions are now being processed directly by CCS/CHS and we have ceased activities with AFTS.

Q. Who did this?

A. We do not know the identity of the individual or individuals responsible for this incident.

Q. Why was I notified?

A. We take the privacy and confidentiality of the information you entrusted to us seriously. While we understand no CCS/CHS donor information is involved in the incident, out of an abundance of caution and in the spirit of full transparency, we opted to voluntarily notify you of the incident. The safety and protection of your information is our highest priority and we recommend you monitor your bank/checking accounts for signs of unusual activity.

Q. Am I affected? I am a donor and heard about a breach but did not receive a letter. Why not?

A. Based on our communications with AFTS, we understand the incident did not impact any CCS/CHS information stored on AFTS' servers. Though not required to notify individuals, we voluntarily notified individuals who made donations to CCS/CHS via paper check and for whom we had current contact information.

Q. Why wasn't I contacted sooner?

A. While the incident occurred on February 3, 2021, we first heard about it from AFTS on February 5, 2021. Upon learning of the incident we immediately started investigating what happened and, though we understand no CCS/CHS donor information was involved in the incident, we voluntarily notified individuals as soon as possible after that.

Q. What specific information may have been compromised?

A. While AFTS's investigation is ongoing and may evolve, we understand no CCS/CHS donor information was involved in the incident.

Q. Did this incident impact CCS/CHS computer systems?

A. No, this incident involves AFTS, a third-party service provider, and did not impact any of CCS/CHS computer systems.

Q. How will I know if my information was used by someone else?

A. At this point, we have no reason to believe your information was involved in this incident and we have not been informed of any incident where fraud or identity theft has occurred as a result of this incident. However, the safety and protection of your information is our highest priority, which is why we, out of an abundance of caution and in the spirit of full transparency, opted to voluntarily notify you of the incident. We recommend you monitor your bank/checking accounts for signs of unusual activity.

Q. I've experienced identity theft and I think it is linked to this incident. What should I do?

A. If you have not done so already, you should report the situation to your relevant financial institutions and to law enforcement authorities, including the police and the attorney general for your state.

In addition, we ask that you notify CCS/CHS by calling (206) 566-6677.

Q. Was this intrusion reported to law enforcement?

A. Yes, we have been informed that AFTS has notified law enforcement.

Q. Do you suspect that my information has been used fraudulently? Has anyone been adversely affected as a result of this incident?

A. At this point, we have no reason to believe your information was involved in this incident and we have not been informed of any incident where fraud or identity theft has occurred as a result of this incident.

Q. What steps do I need to take to protect myself?

A. At this point, we have no reason to believe your information was involved in this incident and we have not been informed of any incident where fraud or identity theft has occurred as a result of this incident. However, the safety and protection of your information is our highest priority. To that end, we recommend that you review your banking/checking account information on a regular basis and report any suspicious activity to the relevant financial institutions and to CCS/CHS.

Q. Will you provide me with complimentary credit monitoring?

A. We are not providing credit monitoring. To our knowledge, this incident did not impact CCS/CHS donor data; therefore, there should be no risk of identity theft.