ID THEFT CASE STUDIES

These four case studies are real life examples of identity theft events that current Zander members have been faced with. They represent non-financial fraud that cannot be detected through credit or ID monitoring programs.

1. EMPLOYMENT FRAUD

A member was notified by the Social Security Administration that income earned was detected under her Social Security Number (SSN) and that the members Supplemental Security Income (SSI) benefits could be affected by the information detected. The member has never worked because she is disabled.

The recovery department contacted both of the employers that reported income earned under this member’s SSN and confirmed that employment was obtained fraudulently. The recovery advocate learned that the member’s SSN was used in conjunction another name to apply for the job. The recovery advocate was able to provide proof of ownership of the SSN to the employer. Upon completion of the investigation, the employers marked their files for fraud to prevent further employment of the identity thief and agreed to never report the income earned again. The recovery advocate secured letters from the employers detailing the fraud that occurred and the corrections have been made with the Social Security Administration. To prevent any tax returns from being filed fraudulently using the member’s SSN, the recovery advocate helped to notify the IRS of the fraud that occurred and to flag the member’s tax file.

2. MEDICAL IDENTITY THEFT

A member received a telephone call from a local hospital seeking payment for Emergency Room visit, apparently made by her. The hospital provided her with the day, time, and services rendered to further clarify the reason for their call. The member had never been a patient at that hospital.

The recovery team contacted the hospital to notify them of the fraud in order to avoid any negative consequence to the member’s health and care. After we collected and provided documents to the hospital staff proving that the signature given to accept their services was in fact a forgery, and not that of our member, her personal information was extracted from the medical records at the facility. She was also relieved of financial responsibility on the account and was provided with documentation stating the corrections made. To assure that her credit remains unaffected, a fraud alert was placed and a related inquiry was removed from her files.

3. INSURANCE FRAUD

A member received EOB’s from her health insurance provider. After verifying the services that she did receive and that were being processed for payment, she was to question five claims she did not recognize. Four claims were submitted by a single provider and a single claim by another. She had never been to the offices of these providers, not even as a legitimate patient. They were billing her insurance for services, which she never signed for or received. When the member reported the fraud to her insurance company, she received resistance and did not receive the assistance needed to resolve the situation.

Our ID Theft recovery advocate contacted the provider to further explore the steps that were to be taken in order to resolve the insurance fraud case and to stop future attempts to utilize the member’s insurance information. The advocate worked closely with the insurance company and was able to have a flag placed onto the member’s account so that further attempts to submit fraudulent claims would be caught immediately. The advocate also had the claims adjusted and the member was relieved of all financial responsibility. The funds that were to be dispersed to the providers were pulled back and the claims were removed from her records.

4. RENTAL FRAUD

A member received a telephone call from an apartment community to confirm a rental application submitted in their name and using their social security number, without their knowledge or authorization. The member denied submitting the application and contacted the recovery department immediately.

The Recovery Advocate contacted the apartment community that same day and learned that the member was contacted by the leasing agent performing the credit check as a result of a fraud alert already in place on the member’s credit file. The recovery advocate provided documents proving the real identity of the applicant listed resulting in the denial of the application. This assured that no lease agreement was created. After reviewing the victim’s credit files, additional rental applications were discovered by the recovery advocate in the form of hard inquiries placed as a result of credit checks performed by two other apartment communities.

The recovery advocate notified the other two apartment communities of the fraudulent rental applications processed. It was learned that one of the units was actually rented to the identity thief currently occupying the space. With the assistance of the recovery advocate, the lease agreement was voided and the member relieved of any responsibility. A police report was filed, and law enforcement made an arrest.