DATA COMPROMISE CASE EXAMPLES

Identity thieves used card skimmers at a gas station to steal bank account numbers with PIN codes from 550 customers. The thieves then created false debit cards, using the stolen information at ATMs to drain funds from client accounts.

–– **Cost of notification and services: $19,250**

Three external back-up hard drives with private personal records for 300 patients were stolen from a locked physician's office. Notifications were sent to affected individuals advising them to place a fraud alert with credit bureaus and to monitor their credit reports and other financial statements.

–– **Cost of notification and services: $10,500**

A burglar broke into an accountant's office and stole a computer with the tax records of 800 clients. The accountant's clients were in four states and the owner needed assistance complying with the variances of state notification requirements. Clients were urged to contact their banks and place fraud alerts on their credit files.

–– **Cost of notification and services: $28,000**

A box of rental applications with the name, address and Social Security numbers of 2,600 individuals was stolen from an apartment building office.

–– **Cost of notification and services: $91,000**

An employee of an investment advisor company installed peer-to-peer file sharing software on a company computer. Identity thieves manipulated the peer-to-peer software to access the private investment records of 2,000 clients.

–– **Cost of notification and services: $70,000**

IDENTITY RECOVERY CASE EXAMPLES

A physician reported being sued for $13,250 due to unauthorized accounts that had been opened in his name when an unauthorized person used the insured's personal information to rent several items and open lines of credit. Our case manager consulted with the insured and placed fraud alerts. The insured hired an attorney to help resolve the issues.

–– **Covered cost of attorney fees: $5,652**

The insured discovered that someone had attempted to open a fraudulent bank account in his name and access $20,000 from his line of credit. The insured lost 15 hours from work in discussions with the bank and police. The fraud attempts were unsuccessful but did create some identity theft related history on the insured's credit reports. Our investigator disputed the unauthorized account history on the insured's behalf and the credit reports were returned to pre-theft status.

–– **Covered cost of lost wages: $865**

Business owner reported that a former employee changed personal information on the business line of credit and attempted to steal money from the insured's company. We assisted the owner, who missed time from work to handle this issue, with restoring his personal information.

–– **Covered cost of lost wages: $5,000**

Business executive reported that an unauthorized account had been opened using his Social Security number. Insured was concerned that the thief would also use his business information and hired an attorney to correct this issue.

–– **Covered cost of attorney fees: $1,018**

CYBERONE CASE EXAMPLES

A transportation contractor was hacked by a former employee, whose passwords had not been changed upon termination. The insured's computer system began to act erratically, crucial software programs were unavailable and large amounts of data appeared to have been deleted.

An outside IT firm was hired to recover electronic data and input other records only available in paper form. In addition, the IT firm reinstalled software, re-configured the insured's servers and repaired other damage to the insured's computer system. The insured also had to replace various pieces of cargo tracking software that had been damaged or destroyed.

Separately, the insured suffered a business income over the course of several days while systems issues were being addressed. The insured also hired a public relations firm to help it communicate with its customers about the incident.

–– **Total First Party Costs: $33,850**

A retail business suffered a virus infection that corrupted data and caused the insured's computer system to stop functioning properly, resulting in loss income. The insured hired an IT firm to remove the virus and reinstall software.

–– **Total First Party Costs: $22,000**

The customers of an insured equipment dealer began to receive strange email messages that appeared to have come from the firm. The firm's owner called an outside IT consultant who investigated and confirmed the insured's computer had been infected by a virus. The virus was removed by the IT vendor.

Several weeks later, the dealer received a certified letter from a local lawyer alleging that a former customer of the equipment dealer had been infected by a virus received in an email message sent by the dealer. According to the letter, the former customer had suffered a variety of different kinds of harm related to the virus and had incurred significant cost to have the virus removed.

–– **Total First and Third Party Costs: $48,200**