03/13/2013

By: Administrator

We read with interest a report earlier this year from Identity Theft 911, an identity theft service provider, concerning complaints that it received from subscribers about unauthorized purchases made through the online Apple store. The fraudsters apparently took advantage of an offer to provide consumers with “instant credit” through Barclaycard.

How did they do it? They used the names of innocent victims plus their birth dates, addresses, Social Security numbers, employers and email addresses to fill out the form for the instant credit. We don’t know how they got that information, but it’s the type that’s often exposed when retailers, employers or government agencies experience data breaches.

When the requests for credit were approved, the scammers returned to the online Apple store, where the new credit card account information was automatically filled in. They placed their orders and directed the shipping to addresses that did not belong to the victims.

Some online merchants don’t allow orders to be shipped to addresses that aren't the same as ones that the bills go to, but others are more flexible. There *are* legitimate reasons why someone might want to use a different address for shipping. For instance, it might be gift and the purchaser wants it to be shipped directly to the person for whom it is intended. Or the purchaser may have more than one home, or wants the item to be shipped to his or her work address. One staff member here at Consumer Federation of America has orders shipped to her husband’s business address because delivery services can’t find her house, which is tucked behind other houses on the street.

How can this type of identity theft be prevented? Creditors can take extra steps to try to verify that applicant *is* the person that he or she claims to be – which is an especially good idea when instant credit is offered. For instance, the credit application can ask questions such as “what is the amount of your monthly mortgage payment,” which only the real person is likely to know. The answer that the applicant provides can be compared to the information in the person’s

credit record to see if it matches. The creditor can also try to call the person, using a phone number from the credit record or another independent source, to confirm whether the application is legitimate.

How can you protect yourself? One thing you should do is check your credit records free once a year to see if there are any accounts that you never authorized. You may be entitled to additional free copies under state law; ask your state or local consumer protection agency. For a fee, you can subscribe to a credit monitoring service that provides alerts about new activity or changes in your credit record.

You can also preemptively "freeze" your credit record at the major credit reporting agencies. This blocks the creditor from checking your credit record, which in most cases will prevent the scammer from opening a new credit account in your name. You'll have to go through the process of lifting the freeze if you want to apply for credit or do something else that may involve checking your credit report (for instance, some landlords and employers check credit reports as part of the application process), and you won't be able to get instant credit, but that's a small price to pay for the peace of mind that a freeze can offer. Some states limit the fees that can be charged in connection with freezes.

And don't just throw mail away that looks like junk – it could be a bill for a purchase that you never made. If it is, contact the company that it came from immediately. If you think you are an identity theft victim you can place a fraud alert on your credit report, which should make it harder for the scammer to open additional accounts in your name.