Ohio Attorney General's
Consumer Advocate
Newsletter
JULY 2015

July 2015

Major National Settlement with Credit Reporting Agencies

Ohio Attorney General Mike DeWine and 30 other state attorneys general recently announced a major settlement with the three main credit reporting agencies — Equifax Information Services LLC, Experian Information Solutions Inc., and TransUnion LLC. Under the settlement, the credit reporting agencies have agreed to make a number of changes to their business practices to benefit consumers.

"The settlement will help protect consumers from credit reports that are wrong, out of date, or even mixed up with someone else's report, and it will reduce the chance that a consumer is wrongly denied a house loan, a car loan, or even a job, because of an inaccurate credit report," Attorney General DeWine said.

The settlement is the result of a multistate investigation that Attorney General DeWine initiated in 2012. The investigation focused on credit report errors, monitoring and disciplining data furnishers (providers of credit reporting information), accuracy in consumer credit reports, and the marketing of credit monitoring products to consumers who call the credit reporting agencies to dispute information on their credit report.

Key provisions of the settlement include:

Higher standards for data furnishers:

- The credit reporting agencies must maintain information about problematic data furnishers and provide a list of those furnishers to the states upon request.
- The credit reporting agencies and data furnishers must use a better, more detailed system to share data.

Limits to direct-to-consumer marketing:

- The credit reporting agencies cannot market credit monitoring services to a consumer during a dispute phone call until the dispute portion of the call has ended.
- The credit reporting agencies must tell consumers that purchasing a product is not a requirement for disputing information on their credits reports.

Added protections for consumers who dispute credit reporting information:

- The credit reporting agencies must implement a new process for handling complicated disputes, such as those involving identity theft, fraud, or mixed files (in which one consumer's information is mixed with another's).
- Each credit reporting agency must notify the other agencies if it finds a mixed file.
- Consumers may obtain one additional free credit report in a 12-month period if they dispute information on their credit report and a change is made as a result of the dispute.

Limits to adding information to a consumer's credit report:

- The credit reporting agencies are generally prohibited from adding information about fines and tickets to credit reports.
- The credit reporting agencies cannot place medical debt on a credit report until 180 days after the account is reported to the credit reporting agency, which gives consumers time to work out issues with their insurance companies.
- The credit reporting agencies must require debt collectors to provide the original creditor's name and information about the debt before adding the debt information to a credit report.

Additional consumer education:

- The credit reporting agencies must tell consumers how they can further challenge the outcome of an investigation into a dispute, such as by filing a complaint with other credit reporting agencies.
- Each credit reporting agency must provide a link to its online dispute website on the website www.annualcreditreport.com, and the credit reporting agency's dispute website must be free of ads and any marketing offers.

Under the settlements, the credit reporting agencies also will pay the participating states $6 million. As the lead state, Ohio received $460,000 under the settlement.

Consumers who want to learn more or receive help from the Ohio Attorney General's Office should visit www.OhioAttorneyGeneral.gov or call 800-282-0515.

Charity Race Runners and Walkers: Do Your Research!

Participating in 5K, 10K, half-marathon, and marathon races is often a great way to raise money for charities you're passionate about, while also accomplishing fitness goals. However, some scammers use the popularity of these events to trick consumers – and charities – out of money.

How the Scam Works:
Fraudsters create legitimate-looking websites and advertise upcoming races to raise money for "charities." Many of the websites even suggest affiliation with local, legitimate charities by including the charities' logos under the sponsorship information. Additionally, the websites often contain pictures of runners and course maps, which likely have been taken without permission from other race websites.

Consumers are directed to a payment page, where they are prompted to submit credit card information for pre-registration fees. Because scammers usually advertise a significantly lower pre-registration fee compared to the race-day fee, many consumers choose to pre-register. However, once the race day approaches, runners learn that the race was never organized and no refunds will be provided.

Tips for Consumers:

- Prior to registering, contact the venue and confirm the race is scheduled.
- Pay with a credit card, instead of a debit card. Under the Fair Credit Billing Act, consumers can dispute fraudulent credit card charges within 60 days.
- Be sure to review the race's terms and conditions. Will refunds be provided if the race is canceled due to weather conditions, etc.?
- If the race website suggests affiliation with a charity, contact the charity to confirm its involvement with the race. Also, contact the Ohio Attorney General's Office to research the charity.
- Conduct an online search by typing the race name and "scam" or "canceled" into a search engine.

- Evaluate the legitimacy of the race website. In addition to registration fee information, most legitimate race websites also provide a course map, parking information, check-in time and event schedules, team names, information about the cause, and photos from past events.

Consumers who believe they have encountered a scam or unfair business practice should contact the Ohio Attorney General's Office at 800-282-0515 or www.OhioAttorneyGeneral.gov.

July 15: Celebrate Military Consumer Protection Day

In recognition of Military Consumer Protection Day (July 15), the Ohio Attorney General's Office is providing information about consumer rights and scams targeting service members and their families.

Unfortunately, a number of factors make service members and military families particularly vulnerable to scams. Members of the military receive steady paychecks, and many members face frequent deployments and relocations. As a result, scam artists often target military families.

In 2014, the Ohio Attorney General's Office received 792 complaints filed by active service members or their immediate family regarding a wide range of consumer issues, including motor vehicles, debt collection, and identity theft. In an effort to resolve these complaints, the office offers an informal dispute resolution process. During this process, a complaint specialist will work with the business and the consumer to try to help resolve the complaint.

One of the common scams targeting service members and their families is called "phishing." Phishing occurs when a scammer unexpectedly contacts a potential victim, pretends to be a trusted person or entity, and requests personal information. Scammers often use this tactic to gather information needed to commit identity theft. To avoid falling victim to this scam and identity theft, never provide personal information to someone who has contacted you unexpectedly.

A recent example of a phishing attack targeted active service members and military retirees through an email pretending to be from the United Services Automobile Association (USAA). The email contained the subject line "Deposit Posted." It contained a file that, once opened, would provide access to personal information. Other attacks directed at U.S. military installations use official-looking emails that appear to come from a senior officer or other authority figure to instruct the recipient to download and install malicious software.

To reduce the chance of becoming a victim of identity theft, active duty members can place an "active duty alert" on their credit report by contacting each of the three credit reporting agencies. This will inform each credit reporting agency that the service member is currently deployed and so should not be opening new lines of credit for a period of time. If an identity thief attempts to open a line of credit in the service member's name, the service member is notified immediately.

Service members also have rights related to payday loans. A payday loan refers to a cash advance secured by a personal check or electronic transfer. These short-term loans often carry large fees and high interest rates. By law, payday loans offered to service members and their dependents cannot exceed the annual percentage rate of 36 percent.

Lastly, military members and families who donate to charities designed to help veterans should be wary of "affinity scams." In this type of scam, a con artist either pretends to represent a trustworthy organization or claims to be a veteran to convince victims to donate money to the cause. Although the scammer claims the money will help veterans, it usually will benefit only the scammer. Before donating to any charity, do your research by contacting the Ohio Attorney General's Office and the Better Business Bureau.

Even if you are not a member of the military, you should be aware that scammers sometimes contact potential victims, claim that they are in the military and need money to get out of trouble. Similar to the popular "grandparent scam," scammers are impersonating military members to try to get victims to send money.

Consumers who believe they have encountered a scam, unfair business practice, or identity theft should contact the Ohio Attorney General's Office at 800-282-0515 or www.OhioAttorneyGeneral.gov.

Are you password protected?

Today, passwords are needed for everything from email to bank accounts. Strong passwords are essential to protecting your information and your money. On the other hand, weak passwords can unlock a treasure trove of both personal and financial information about you for anyone to see.

A strong password is one that is difficult for hackers and scammers to guess. A weak password is one that is easy to guess. Examples of commonly used weak passwords are "123456" and the word "password." While both of these passwords are easy to remember, they also are easy to guess.

To create a complex password, use at least eight characters and a combination of upper and lower case letters, numbers, and symbols. Also, stay away from easy-to-guess passwords, such as your child's name, birthdate, or address.

An easy way to create a complex password is to use the first letter of each word in a familiar phrase, and add a number at the end. For example, if you used the phrase, "I married my wife Sally in 1985!" your password would be, "ImmwSi1985!" Now you have a password that's easy to remember but hard for potential hackers to guess.

Never use the same password for multiple websites. If a hacker discovers a password used for one account, the hacker could use that password to access other accounts that use the same password. Additionally, it may be helpful to keep passwords written down, but be sure to store them in a safe place away from your computer.

In addition to creating strong passwords, consider using "two-factor authentication" to help protect your accounts. Two-factor authentication requires a password and another step to verify your identity. For instance, some websites require a password and then an answer to a question, such as "What is your current zip code?" This adds a second line of defense.

Along with passwords, mobile device passcodes are extremely important. Many people keep valuable information on devices such as cell phones and tablets. While these portable devices are convenient, they can easily be misplaced or stolen. Putting a passcode on your device will help protect your information should it ever become lost. Also, be leery about storing passwords electronically, especially on mobile devices.

Below are some additional tips to protect yourself:

- Never give your password to anyone, especially someone who contacts you unexpectedly. Scammers may "phish" for your passwords by calling and pretending to be your bank or a government agency. Know that these entities will likely not call you requesting your password.
- If you learn that your password has been breached, change your password on other sites where you use the same password. Remember to use a different password for each of your accounts.

- Update your passwords regularly. This could be as simple as changing the numbers at the end of the password, but keep in mind that passwords shouldn't remain the same forever.

If you believe you have encountered a scam or unfair business practice, or if you have been the victim of identity theft, contact the Ohio Attorney General's Office at 800-282-0515 or www.OhioAttorneyGeneral.gov.