

Fraud Victims Can File Claims for \$586 Million Western Union Fund

Consumers who sent money to scammers using Western Union's wire service between 2004 and early 2017 may now apply for compensation from a \$586 million fund. The fund is related to a settlement that Ohio Attorney General Mike DeWine announced in January.

You may be eligible to receive compensation if you lost money to a scam and sent the money through Western Union between Jan. 1, 2004, and Jan. 19, 2017. The fund is held by the U.S. Department of Justice's victim asset recovery program.

Attorney General DeWine announced the claims availability in November, saying "it's not often that scam victims have a chance to recover some of their money, so we want people to know about this opportunity. If you think you're eligible, file a claim."

A settlement administrator is sending claim forms to over 500,000 consumers. You may receive a form in the mail if you reported to Western Union or to the Ohio Attorney General's Office that you had been the victim of a scam using Western Union. The form will contain instructions on how to file a claim.

If you do not receive a claim form but believe you may have a valid claim, visit <u>www.WesternUnionRemission.com</u> or call 844-319-2124 for details on filing a claim.

Completed claim forms must be submitted online or mailed back to the settlement administrator by Feb. 12, 2018.

In January, Attorney General DeWine announced a multistate settlement with Western Union requiring the company to develop and put into action a comprehensive anti-fraud program designed to help prevent consumers from wiring money to scam artists. The agreement was related to a federal settlement in which Western Union agreed to pay \$586 million to provide refunds to victims of fraud-induced wire transfers.

Medicare Recipients to Receive New ID Cards

Older adults across the nation are expected to receive new Medicare cards by April 2019. With this update, it's important to know what to expect and to be on the lookout for con artists trying to steal money or personal information.

If you receive Medicare, you should expect to receive a new Medicare card in the mail between April 2018 and April 2019. The card will have a new, randomly assigned Medicare number instead of your Social Security number. You will not need to pay for the new Medicare card. The card will come to you automatically; no one who truly represents Medicare will call you to ask for money or to verify your personal information to get this new card.

Medicare.gov, the program's official government website, has highlighted a few scams related to the new card distribution. Beware of:

- Someone calling you wanting to confirm your Medicare or Social Security number in order to issue you a new card. (The real Medicare program will *not* call to confirm your Social Security number. Also, it will use your mailing address on file with the Social Security Administration.)
- Anyone trying to charge you for the new card and wanting to verify personal details. (The real card is free and will be mailed to you automatically.)
- Someone claiming your Medicare coverage will be canceled unless you provide personal information such as your Medicare number.

Even though the new Medicare card will no longer include your Social Security number, it is still important to treat this card as you would treat any other sensitive personal information. Medical identity theft occurs throughout our country, and it can happen when someone uses your personal information to order medical equipment or procedures without your consent.

To learn more about the new card, visit the official site for the Centers for Medicare and Medicaid Services at https://www.cms.gov/Medicare/New-Medicare-Card. If you suspect a scam or an unfair business practice, contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Three Things to Know About Credit Alerts and Freezes

In light of recent large-scale data breaches, it is more important than ever to know the steps to take to protect your identity. That includes understanding the different alerts and freezes you can request from the major credit reporting agencies.

Here are three things to know about credit alerts and freezes:

1. An initial fraud alert is free and lasts 90 days.

You can place an initial fraud alert on your credit reports by contacting one of the three major credit reporting agencies — Experian, Equifax, or TransUnion. The agency you choose is responsible for contacting the other two agencies. This alert will act as a red flag to new creditors that your identity may be at risk and to verify your identity before opening a new credit card, loan, or other financial product in your name.

The initial fraud alert will stay on your credit report for 90 days but can be renewed indefinitely. The alert is free, will not affect your credit score, and will make it more difficult for someone to open credit in your name. You do not have to be a victim of identity theft to place an initial fraud alert.

2. An extended fraud alert can help protect identity theft victims.

An extended fraud alert is typically available only to identity theft victims. The extended fraud alert is free, will not affect your credit score, and will essentially act like an initial fraud alert but for a period of seven years.

When you have placed an extended fraud alert, you are eligible to receive two free credit reports from each of the credit reporting agencies within 12 months of placing the alert. (Note: If you have asked a credit reporting agency to make corrections to your credit report, it can take up to 90 days for the agency to make changes.)

Also, with an extended fraud alert, your name will be removed from credit card companies' marketing lists, so you won't receive prescreened credit card offers for five years (unless you wish to add yourself back to those lists).

3. A credit freeze helps "lock" your credit and may cost \$5 per freeze.

In Ohio, you can place a credit freeze on your credit report with any or all three major credit reporting agencies. Parents also can <u>freeze their child's credit record</u> to help guard against child identity theft.

A credit freeze essentially puts a lock on your credit, so new creditors can't access your reports. This helps protect you from unauthorized accounts being opened in your name. A credit freeze does not block unauthorized charges to your existing credit cards, so it's still vital to closely review your account statements. Existing creditors – and debt collectors working on their behalf – can still access your credit reports.

Placing a credit freeze on your account also entitles you to one additional free credit report from each of the credit reporting agencies from which you have requested a freeze.

You do not have to be a victim of identity theft to institute a credit freeze, and a freeze will not impact your credit score.

In Ohio, security freezes are permanent until you lift them. You can be charged a \$5 fee per credit reporting agency to place or remove a freeze. This fee is waived for victims of identity theft, and currently Equifax is waiving the \$5 credit freeze fee. To freeze your report you must contact each credit reporting agency individually.

Private products

Some credit reporting agencies currently offer or plan to offer their own products that contain a "lock" feature designed to block access to your credit report. It is important to evaluate these products with the understanding that, unlike credit freezes, they are not specifically regulated by state law.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at <u>www.OhioProtects.org</u> or 800-282-0515.

Ohioans Report Grant Scam Phone Calls

Consumers across Ohio are reporting scam phone calls about phony grants, especially by con artists pretending to work for government agencies.

In 2017, the Ohio Attorney General's Office has received approximately 400 reports of suspected grant scams. Additionally, more than 50 consumers have reported losing \$200 to \$48,000 to the ploy.

In a typical grant scam, consumers receive a call saying they have won a federal grant of \$7,000 to \$10,000. In order to receive the grant, they must first send a few hundred dollars to cover taxes, insurance, or other costs. Money must be sent via wire transfer or a prepaid money card. In reality, there is no grant; the call came from a con artist.

At the national level, the Federal Trade Commission reports that con artists impersonating the National Institutes of Health claim there are \$14,000 grants available for consumers who pay a fee through a money card, iTunes gift card, or by submitting their bank account number. In reality, as the FTC explains, the federal government will not call you to give you a grant. NIH does grant money to researchers, but they must request the funding and use it for the public's benefit.

Consumers who send money once will often be contacted again, with the scam artist claiming that the consumer needs to send more money for additional costs. The scammer will likely continue

calling as long as the consumer keeps sending money.

Scam artists may give the following phony justifications as to why a consumer has been selected for the grant:

- "You deserve it."
- "You're a good citizen."
- "You haven't had any recent arrests."
- "You're current on your taxes."
- "You have good credit."

To protect yourself from grant scams, never make an upfront payment in order to receive a grant. Be especially cautious any time payment is requested via wire transfer, money order, or gift card. Also keep in mind that true government grants typically are awarded to organizations, not to individual citizens, and information about legitimate federal grants is available for free at <u>www.Grants.gov</u>.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at <u>www.OhioProtects.org</u> or 800-282-0515.