

Protecting Against Immigration Fraud Schemes Targeting Foreign Nationals

March 5, 2019

Foreign nationals should take steps to protect themselves from fraudulent immigration schemes and websites falsely claiming to be affiliated with the U.S. government.

In the current climate of heightened immigration focus, foreign nationals are increasingly vulnerable to immigration fraud. Unscrupulous individuals seek to take advantage of this vulnerability, using sophisticated methods to obtain money or personal information.

Foreign nationals must be vigilant against such schemes, which are widespread. The following are some guidelines to help identify and protect against common immigration scams.

AVOID WEBSITES POSING AS OFFICIAL GOVERNMENT SITES

There are numerous websites posing as official government sites or claiming to provide immigration benefits with U.S. government authorization. Unless a website contains a “.gov” suffix, it is not an official U.S. government site.

- **Visa Waiver Program websites.** If you are planning business or pleasure travel to the United States under the Visa Waiver Program (VWP) and need to register in the Electronic System for Travel Authorization (ESTA), make sure to use U.S. Customs and Border Protection’s official ESTA website at <https://www.cbp.gov/travel/international-visitors/esta>. Avoid websites that offer to submit ESTA applications for additional fees. These are not authorized by the U.S. government and may be fraudulent.
- **Diversity Visa Lottery websites.** If you are planning to enter the annual Diversity Immigrant Visa Lottery (DV lottery), make sure to use the official [State Department website](#) to submit your application. Avoid commercial DV lottery websites that charge a fee. Be suspicious of any website or communication claiming that you have won the lottery. The official lottery site is the only legitimate source to learn whether you have been selected in the lottery; the State Department does not contact winning lottery applicants by mail, email or fax. Click [this link](#) for more on protecting against DV lottery fraud.

PROTECT YOURSELF FROM FRAUDULENT PHONE AND EMAIL SCHEMES

In a common immigration-fraud scheme, you may receive a phone call or email from someone who purports to be an official of U.S. Citizenship and Immigration Services or the Internal Revenue Service. The individual may claim that there is a problem with your immigration or tax records and demand money or information. These calls are typically fraudulent.

If you receive a call claiming to be from a U.S. government official, protect yourself as follows:

- **Do not forward funds.** The IRS and USCIS never solicit payment via telephone or email. Be especially suspicious of a caller who demands unconventional payment methods such as store gift cards.
- **Do not provide sensitive personal information over the phone unless you are sure the call is legitimate.** Do not provide or confirm personal information, such as a Social Security Number, I-94 number, birth date, or passport number, unless you are sure you are speaking with a government official (see below). If you are doubtful, ask for the caller's name and call-back number; a perpetrator will typically hang up.
- **Do not be fooled by misleading caller ID information.** A common scheme involves displaying the caller ID as "U.S. Immigration," "911," "USCIS," or the IRS. Do not rely on a caller ID to verify a caller's identity.
- **Do not succumb to threats.** Scammers may grow increasingly hostile when you do not cooperate, threatening to arrest or deport you, or suspend your business or driver's license. They may even send follow-up emails or calls from accomplices claiming to be from the local police or the Department of Motor Vehicles. These threats are illegitimate.
- **Learn how to recognize a legitimate government communication.** There are circumstances when a U.S. government official may legitimately contact you. If you called USCIS's National Customer Service Center or contacted IRS customer service, an officer may return your call. You or your employer may receive a phone call, email or in-person visit from an officer of the USCIS Fraud Detection and National Security (FDNS) unit, which routinely investigates employment-based immigration petitions. If you are uncertain about the legitimacy of a call, email or visit, ask for verification. A legitimate government official will always be able to provide you with a name, official identification and a functioning phone number.

WHAT TO DO IF YOU SUSPECT FRAUD HAS OCCURRED

- If you have already transferred funds or provided personal information, monitor your credit report and credit card accounts after filing a complaint with local law enforcement and other appropriate authorities.
- Inform your employer's human resources or immigration representative, or your Fragomen professional.
- Contact the appropriate government agency to make a report; see below for contact details.

ADDITIONAL RESOURCES FOR VICTIMS

Various government agencies offer guidance on how to protect yourself from common immigration-fraud schemes and how to report fraud.

- [USCIS](#) offers detailed information on common immigration scams and how to report them.

- The [IRS](#) provides guidance on recognizing common tax scams and fake IRS communications.
- The U.S. [Federal Trade Commission](#) provides consumer protection information for victims of immigration fraud.
- The [Department of State](#) advises on common Diversity Visa lottery scams.

If you have any questions, please contact the immigration professional with whom you work at Fragomen.