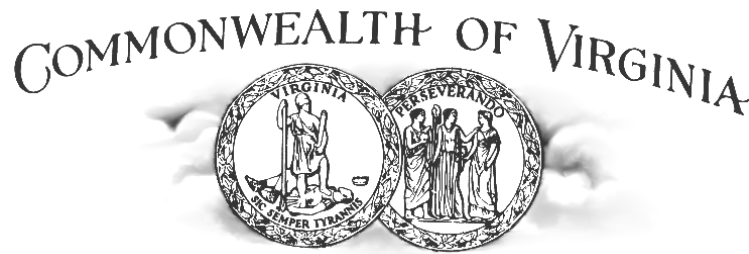


E. J. FACE, JR.
COMMISSIONER OF
FINANCIAL INSTITUTIONS



Mailing Address:
P.O. BOX 640
RICHMOND, VA 23218-0640

(804) 371-9657
FAX (804) 371-9416
scc.virginia.gov

Physical Address:
1300 East Main Street, Ste 800
Richmond, VA 23219

STATE CORPORATION COMMISSION BUREAU OF FINANCIAL INSTITUTIONS

Scam Prevention – Fake Website Scams

The old saying “if it sounds too good to be true, it probably is” should be on your mind when reviewing websites.

Scams involving phony websites and fake online businesses are prevalent. It is easy to create a website from anywhere in the world. Scammers can add a few fake “positive reviews” and a fake street address – or even copy the actual street address of an unsuspecting business – and then sit back and wait for the money to roll in. The unsuspecting consumer believes the website and address is a “real” business and submits an online payment or wire transfer.

Unfortunately, because the fake business exists only online, the scam artists are extremely difficult, if not impossible to track. The unsuspecting consumer is out of their money, which typically is not recovered, and is also subject to identity theft if personal information was provided to the scammer. The scam artists then move quickly, shutting down the website and creating a new fake business.

Red Flags and Warning signs to check before contacting the company or providing any information:

- In Virginia, check to see if the company registered with the State Corporation Commission (SCC) as a business entity, many (but not all) businesses operating in Virginia require a filing of their business information with the SCC’s Clerk’s Office. If the company offers loans, check to see if the company is licensed with the Virginia Bureau of Financial Institutions (BFI). A quick online search of businesses registered with the SCC, or financial institutions licensed with the BFI, can be found at: scc.virginia.gov.
- Be sure to check out the street address listed for the company by using an online mapping program, click on “street view” to actually see what is located at that address. Helpful information about an address can also be found by doing a quick search under “Find a Zip Code” on United State Postal Service website at usps.com.
- If you are asked to send or wire money, buy prepaid cards, or money orders, etc., **STOP!** Sending money in advance is often a sign of a scam especially using the methods listed above which are often untraceable.
- Don’t trust your caller ID if they are calling you. Readily available technology makes it easy to create a fake name and number to display on caller ID or as the “sender” of a text message.

If you are the victim of a fake business scam:

- Report the scam to the FBI’s Internet Crime Complaint Center at www.ic3.gov
- Report the matter to your local police (non-emergency number)
- If you provided your bank account or credit card information report the matter to your financial institution
- If you provided personal information such as your date of birth, social security number, etc. consider placing a fraud alert on your credit file. The Federal Trade Commission has information on how to do this at: <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>