Customer Security and Fraud Awareness

Our Approach to Security

At VFX Financial security is our top priority and when you access your account. Here are some of the ways we do that to help keep you safe when transacting with us online:

Your Login Details – we provide you with account login credentials unique to you. You must not share them with anyone else.

The Login Process – Two Factor Authentication provides an additional layer of security to your account. It requires two successive forms of authentication: - 'something you know' such as your account number and password, and 'something you have ', such as the number associated with your mobile device, or "something you are", such as a biometric sign-in.

Account Questions – If you contact our customer services team, we will ask you to confirm your identity by asking you certain questions related to your account. We will never ask for your PIN or password.

One Time Passcodes or push messages – We may send unique one time use codes or push messages to your registered devices when additional security and validation is required, for example:

- when you make payments from your VFX account;
- periodically when you login, just to make sure it is you;
- When you make changes to your personal details; or
- When you contact our customer services team by telephone.

Providing Information – While speaking to VFX over the phone, by chat, or email we will never ask you for your password or PIN number. Please do not respond to emails that appear to come from VFX asking you to confirm your login details or any other details which might be used to gain unauthorised access to your account. Also, do not click on any links that they may contain.

I

Fraud

If we suspect that fraudulent activity has taken place on your account, we may temporarily block your account and contact you for further information. We will contact you in accordance with your communication preferences configured on your account which may include email, telephone and in-app PUSH message.

How to Report Fraud

If you notice something suspicious and believe it could be fraudulent, you should contact us as soon as you become aware of it by contacting VFX Customer Services: support@vfxfinancial.ca or call: +1 (416) 613 0260.

Suspicious Emails: Fraudsters my try to initiate or emails and email addresses. If you receive an email asking you to provide any personal details, or your login details please forward the email to email address and then delete it. **Do not respond to the email or click on any links that it may contain**.

How to Protect Yourself from Fraud

Help to keep yourself safe from fraudsters by following the tips below. Remember, if you are ever unsure, contact VFX Customer Services.

To help us, please make sure your mobile telephone number and email address registered with us is up to date. We will use these to contact you if we notice unusual activity on your VFX account.

Tips for Staying Safe Online

When accessing your account online;

- Use up to date antivirus software and firewall.
- Make sure you keep your computer and browser up to date.
- Use secure networks, a guest wireless network such as those in a hotel may not be secure.
- Use strong passwords and change them regularly.
- Don't share your password including one-time passwords sent to you.

When using a mobile application;

- Only install apps from recognised app stores.
- Consider the app ratings and reviews.
- Be aware of what permissions you are granting.
- Treat your phone in the same way that you would treat your wallet or purse.

When shopping online;

- When using an online retailer for the first time, do some research to make sure that they are genuine.
- Do not reply to unsolicited emails from companies you don't recognise.
- Before entering your prepaid card details, make sure the link is secure. There should be a padlock symbol in the browser frame window which appears when you login or register, if this appears on the page rather than the browser it may

indicate a fraudulent website. The web address should begin with https://, the 's' stands for secure.

- Always log out of website after use. Simply closing your browser is not enough to ensure your data is safe.
- Keep your PIN safe and do not share it.
- When entering your PIN, check for people around you and hide your PIN number.
- Always check your account statements.

Remember, if you decide to donate, resell or recycle your mobile phone, computer, laptop or tablet, make sure you fully remove all data and apps first, as otherwise these may be accessed by whomever your device is passed on to.