Below are some reminders to help keep you and your financial information safe. You will not likely find a foolproof way to prevent identity theft or fraud, but hopefully these important guidelines will stick in your head.

- Don't give out personal information! Identity thieves attempt to pose as a bank or credit card company. If you think about it, those places already have your information, they may only need to verify part of it. Be alert to phishing and spoofing attempts. Phone calls can be made to appear to come from anywhere. So, emails and calls that appear to come from government entities and legitimate business may be scams. If you question something, ask to initiate a callback or return the email yourself. Then find contact information from a trusted source (your records or website) and call them to verify whether the call or email is legitimate. You may be told you have won something or that you are in danger of being arrested. Most credible places to not initiate contact with taxpayers by phone (or email or social media) to request personal or financial information, nor does it call with threats of arrest or lawsuits.
- Take your name off marketers' hit lists. In addition to the national Do-Not-Call Registry (1-888-382-1222), cut down on junk mail and opt out of credit card solicitations. OptOutPrescreen.com is the official Consumer Credit Reporting Industry website for consumers to Opt-In or Opt-out from offers of credit or insurance.
- Protect your mobile devices. Mobile devices can be a real risk, only about half of us lock our mobile devices. Use passwords or other authentication options. Also, opt for an app over a mobile browser version, may be safer.
- Skimming is stealing card information using a small device attached on a card reader, commonly a gas pump or ATM. Use cards with chips, which have added protections. Pay inside at the gas station if you can, skimming devices are more likely placed at unmonitored locations. Never leave ATM, credit card or gas station receipts behind.
- Never let your credit card out of sight. Always keep an eye on your card, when not possible pay with cash.
- Don't carry your Social Security card or more credit cards than you regularly use.
- Do not keep a list of passwords or PIN with you.
- Make photocopies of your credit cards in case they are lost or stolen.
- Regularly review your bank & credit card statements. Especially after you've made many online purchases or used a new site. Most times you only have 60 days from when your statement was sent to dispute a charge.
- Watch your mailbox! You may not think of it, but stolen mail is one of the easiest ways to steal an identity. Hold you mail if you're going to be out of town and don't post vacation pictures on social media until you have returned home. Maybe consider a locked mailbox or P.O. box.
- Shred, shred, shred! Any credit card, bank or investment statement is susceptible. Shred junk mail too, especially preapprove credit offers.
- Get electronic statements. You may want to look into secure storage to keep more than your online banking service holds.
- Check your credit reports regularly. The three major credit reporting bureaus which normally give you a free credit report yearly are allowing a free credit report weekly until April 20, 2022. See www.annualcreditreport.com or call 877-322-8228. If you find something, alert your creditor immediately. Accounts in deferment should be checked closely that they are being reported properly.
- Create strong, unique passwords for online accounts. Use a combination of symbols, numbers, letters, caps & lowercase.
- Do not rely on security questions to keep your accounts safe. Your mother's maiden name and pets' names are not hard to find. Think carefully about what you post on social media… those fun quizzes you take and share ask for exactly what you might use as answers for security questions!
- Set up alerts and notifications. VFCU online banking and the mobile app both have those capabilities. On the mobile app, go to 'more' and 'manage cards'. There is also the capability to lock and unlock your cards. In ItsMe247 go to 'Info Center' and 'eAlert subscriptions'.
- Don't use public Wi-Fi for shopping, banking or other sensitive transactions.
- Make sure your connection is encrypted. Most browsers show a connection is secure by having a lock and/or the letters HTTPS in green preceding the website name.
- Do not click on pop-up ads.
- Purchase from websites you know, trust and have done business with previously. If you are contemplating a website you are not familiar with, read the reviews section to get an idea of the company's reputation.
- Avoid suspicious websites and links. Never click or open attachments from someone you don't know, they may contain malware. Emails and websites can easily be spoofed.
- Consider dedicating one card only for online purchases. That way, if compromised, you can change the card without impacting other payments.
- Or try a prepaid card. VFCU offers prepaid debit cards which are not linked to your account and can be loaded with minimal amounts. They have their own online banking and mobile app to help you manage your spending.
- Got a smartphone? Then use a digital wallet. VFCU debit cards are compatible with Google Pay, Apple Pay and Samsung Pay. Use these tokenized and encrypted transactions to shop online or at compatible checkout terminals. Plus, contactless transactions have fewer health risks.
- Find more great resources on our website under -Other Services and Educational Resources.
- If you ever have questions on your card after hours, please call a card service representative at 866-664-9364.