Bank-Fund Staff Federal Credit Union

web secure

http://www.bfsfcu.org/websecure/index.html

# Introduction

## Trust

At Bank-Fund Staff Federal Credit Union, we are committed to protecting your accounts and identity. BFSFCU follows or exceeds industry best practices for securing Internet commerce (known as e-Commerce) related services we provide to our members.

Human beings are trusting in nature; from the newspapers we read to the television we watch and family and friends whose advice we may heed. The Internet was built on trust and to a certain extent, anonymity. In using BFSFCU's e-Commerce services, you have put your trust in us and we want to let you know how we're protecting that trust via security measures implemented to safeguard account and personal information. However, as with any strong relationship, trust must flow both ways, and we hope this guide will serve as a resource for What We Do and What You Can Do to protect yourself from online fraud and identity theft.

Throughout this Guide you will find terms highlighted for which definitions may be found in the Glossary section or by simply clicking on the link to our Frequently Asked Questions (FAQ) section where applicable.

## Online Security

Your online security is our highest priority. And while we are hard at work protecting your member account and the personal information with which you have entrusted us, thieves and hackers are persistent in their efforts to develop newer and more insidious ways to break down the safeguards. As part of our commitment to your online security, we will provide our members with pre-emptive notification, education, and access to useful information.

The following are examples of how an unauthorized user may attempt to gain access to or exploit the e-Commerce systems for personal gain:

- Phishing: a form of social engineering characterized by attempts to gain access or personal information by impersonating a legitimate organization or individual, via e-Mail, instant message, or through a website.
- Pharming: the exploitation of vulnerabilities in the DNS servers that allows a hacker to acquire the Domain Name (e.g. "mycompany.com") for a site and to redirect traffic from that company's legitimate site to the hacker's website.
- Viruses / Trojans: malicious software intended to intercept or take control of a computer's operation without the user's consent. While viruses are typically used to destroy data or harm the computer, some are fairly benign while others are designed to capture personal information and transmit it back to the hacker's web site.
- Spyware / Keystroke loggers: Similar to viruses and trojans, although typically spyware and keystroke loggers are not self-replicating. Used for capturing personal information without the user's knowledge.
- Identity Theft: The exploitation of a successful social engineering attack in which a person deliberately assumes the identity of another person for financial gain.

Please refer to the sections on What We Do and What You Can Do to learn more about how together we can greatly reduce the risks posed by such attacks. In addition, the following links will allow you to learn more about these and other threats:

FBI Fraud Alert
Online Security Frequently Asked Questions
Online Security TEAM Website
OnGuard Online
National Internet Fraud Watch Information Center
e-Consumer.gov
Symantec Antivirus Research Center (SARC)

# Identity Theft

Identity Theft (ID Theft) is one of the fastest growing crimes in the United States and usually occurs when someone uses your name or personal information to open new accounts, initiate transactions in your name, or commit other forms of financial fraud. Identity Theft involves the invasion of privacy and personal information, posing a risk to your good name and reputation. The consequences of ID Theft can be staggering when taking into account the extensive amount of personal time spent by victims in dealing with creditors, financial institutions and law enforcement agencies in tracking down those responsible. Statistics show that victims spend, on average, 175 hours per incident to resolve problems caused by the fraud. Successful ID Theft may lead to credit of loans, jobs, and other services that rely on a credit rating report from one of the three National Credit Bureaus.

Identity thieves exploit any avenue available to gain access to personal information. The following are a few examples:

- ***Group Identity Theft:*** a thief gains access to a repository of personal information for businesses or organizations such as a retail store, fitness center, car dealer, school, hospital, or websites.
- ***"Dumpster diving":*** a thief scours through your trash to find unshredded information, such as credit card offers, bank statements, bills, or personal correspondence.
- ***Someone the victim knows:*** an Identity thief may be someone the victim knows and has trusted with personal information, such as a roommate, landlord, employee or employer.
- ***Stolen wallet or purse:*** a thief may gain access to personal information available on a driver's license, social security card, or credit card. A wallet may contain a wealth of information more valuable to Identity thieves than the limited cash inside.
- ***Intercepting mail:*** a thief may complete a "change of address" and redirect personal correspondence to another location.
- ***Directly from you:*** a thief may pose as a legitimate representative of your Credit Union or bank (or their vendo/partners), employer, government agency, business or landlord who may have valid reason to request such information. They may even use fake e-Mail and websites to try to obtain information from you.

There are numerous resources available for identifying, learning how to protect from, and finding assistance in reporting Identity Theft if you are a victim:

Identity Theft Frequently Asked Questions
Identity Theft Resource Center
FTC Consumer
U.S. Department of Justice
Social Security Administration
USPS Postal Inspectors
Better Business Bureau

November 2005

# Identity Theft Frequently Asked Questions

## What is a secure web site?

A secure web site is a type of web server that is capable of communicating over the internet with a web browser in a secure manner. Normally, the contents of any HTML document, image file, or HTML form, including possibly usernames and passwords, are transmitted over the internet as clear text with no authentication required by the user. A secure web server allows for a safer connection to the browser by establishing a trust between the client and the server in which all communication between the two is encrypted to prevent eavesdropping.

## Is the BFSFCU web site secure?

We meet or exceed industry standard security practices for the secure transmission and storage of your confidential information using 128-bit SSL encryption. In addition, we use safety measures such as Firewalls, Intrusion Detection Systems, Application Layer Filtering, and proactive monitoring to protect your accounts and information. Please refer to the section "What We Do" to learn more about how we help to protect you.

## What is encryption?

Encryption is a process by which we use software to scramble sensitive information while it is in transit to Bank-Fund Staff FCU. Please take a moment to read about the steps that we have taken to help protect your information and make your online transmissions safer in the section labeled "What We Do". We also invite you to review the steps you can take to help protect yourself further in the section labeled "What You Can Do".

## How does encryption work?

Encryption is based on a key that has two different parts; the public part and the private part. The public part of the key is distributed to those you want to communicate with. The private part is for the recipient's use only. When you send personal information to secure.bfsfcu.org, you use BFSFCU's public key to encrypt your personal information. That means, if at any point during the transmission your information is intercepted, it is scrambled and very difficult to decrypt. Once BFSFCU receives your encrypted personal information, we use the private part of our key to decode it.

## How safe is encryption really?

Providing encrypted information via BFSFCU’s secure web site is as safe or safer than doing so over the phone or via fax and exponentially safer than providing confidential information via e-Mail or regular mail.

## What information does BFSFCU encrypt?

Bank-Fund Staff FCU encrypts all personal and financial information that is presented to the members via our internet-based e-Services. In addition, all forms requiring members to enter personal or financial information in order to perform transactions or submit requests (such as change of address) are encrypted to ensure confidentiality and security of the communication. Remember, if you feel uncomfortable providing any of this information online, please feel free to call and speak with one of our Member Services representatives at 1-800-9-BFSFCU.

## What is a cookie?

A cookie is a packet of information sent by a server to a browser and then sent back by the browser each time it accesses that server. Cookies can contain any arbitrary information the server chooses and are used to introduce state into otherwise stateless HTTP transactions. Without cookies, each retrieval of a web page (technically, each component of a web page) from a web site is an isolated event, virtually unrelated to all other views of the site's pages. By returning a cookie to a web server, the browser provides the server a means of connecting the current page view with prior page views. Typically this is used to authenticate or identify a registered user of a web site as part of their first login process or initial site registration without requiring them to sign in again every time they access that site. Other uses are maintaining a "shopping basket" of goods selected for purchase during a session at a site, site personalization (presenting different pages to different users), and tracking a particular user's access to a site.

## So what does a cookie do for me, the member?

Cookies provide several immediate advantages on secure.bfsfcu.org. For example, when using Online Banking, cookies are used to maintain session information and “remember” when a member has authenticated; thus not requiring members to enter their credential information with each transaction request. Cookies also enable the system to track a members “state” on the system and automatically sign them off should their session remain idle for a certain period of time. You may choose to configure your Internet Browser to stop accepting cookies; however, you will not be able to fully experience the interactive features of BFSFCU’s e-Services or those of many other Web sites you visit.

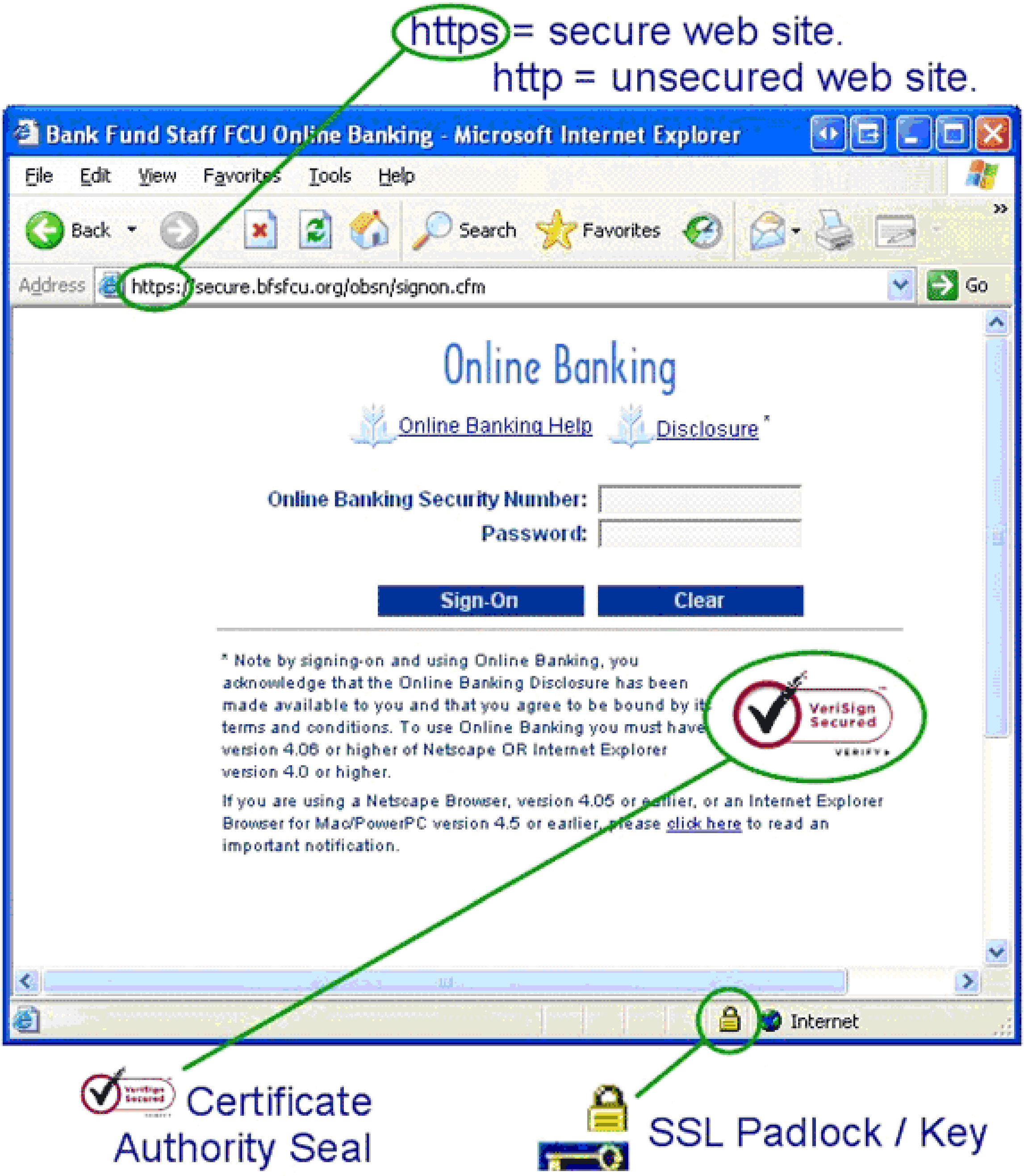
## Why do I need to know this about cookies?

At BFSFCU, we want you to know why we ask you to configure your browser settings to accept a cookie. We want to be sure you understand that accepting a cookie in no way gives us access to your computer or any personal information about you. We know that a lot of people have concerns about cookies, but we feel that the benefit we both gain from their proper use is worthwhile.

## How do I ensure I am using a secure connection to BFSFCU?

The simplest way to ensure that your browser is communicating via an encrypted channel with BFSFCU is to look for a closed lock icon or unbroken key (depending on your browser) on the bottom status bar. These icons serve to indicate that the connection is secured using SSL encryption. You can typically see the level of encryption that has been negotiated between the browser and server by positioning the cursor over these icons. By default Internet Browsers will negotiate the highest level of encryption available to both the server and client browser.

Alternatively, most secure web sites will prominently display a “Seal” (as illustrated below) from the certificate authority on pages requesting personal or confidential information. The certificate authority is responsible for generating certificates used to encrypt communication between your browser and a secure web site and validates that the organization issued the certificate is valid and the rightful owner of the site.



https = secure web site.
http = unsecured web site.

Bank Fund Staff FCU Online Banking - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
https://secure.bfsfcu.org/obsn/signon.cfm
Go
Online Banking
Online Banking Help
Disclosure*
Online Banking Security Number:
Password:
Sign-On
Clear
VeriSign Secured
VERIFY
Internet

* Note by signing-on and using Online Banking, you acknowledge that the Online Banking Disclosure has been made available to you and that you agree to be bound by its terms and conditions. To use Online Banking you must have version 4.06 or higher of Netscape OR Internet Explorer version 4.0 or higher.

If you are using a Netscape Browser, version 4.05 or earlier, or an Internet Explorer Browser for Mac/PowerPC version 4.5 or earlier, please click here to read an important notification.

Certificate Authority Seal

SSL Padlock / Key

In addition, the connection type (secure vs. unsecured) and encryption level is also available from the Internet browser by viewing the properties for the page or sometimes the frame within the page where confidential information is requested.

## How do I know if the web site I am on is really BFSFCU’s web site?

The most effective way to ensure you are really on Bank-Fund Staff Federal Credit Union’s web site is by typing the full URL into your Internet Browser or using a saved bookmark/favorite instead of following a link embedded within an e-Mail or another site. While browsing the Credit Union’s web site or using the Online Banking services, ensure your browser’s address bar shows a connection to “bfsfcu.org” or “secure.bfsfcu.org”. When initiating a secure SSL connection, most Internet Browsers will display a closed lock at the bottom of the browser window indicating a secure connection. By clicking on the lock, you will also be able to view the SSL certificate and thus determine if the site is legitimate.

## What is Phishing?

Many financial institutions and companies that conduct business on the Internet, including Bank-Fund Staff FCU, have become the target of a form of online fraud called "phishing" (sounds like "fishing"). Phishing attacks usually take the form of unsolicited emails or pop-up Web pages. To make the phishing attacks look official, scammers often include image and logos from legitimate companies.

## What is Pharming?

Every web site on the internet has a so-called unique IP Address; much like phone numbers, these IP Addresses identify servers across the global internet and permit the routing of traffic from one network to another. In order to simplify the process of accessing data and information across the World Wide Web, a Domain Naming System (DNS) was established for the assignment and translation of simple names, for example "www.google.com" or "bfsfcu.org" to unique IP Addresses. By manipulating domain naming entries via exploits in DNS servers, hackers attempt to redirect a web site's traffic from the valid IP Address to an alternate site; typically faked to appear legitimate in the hopes of "phishing" for valid authentication credentials and/or personal information such as e-Mail addresses.

## What is e-Mail fraud?

E-mail is a convenient and affordable way to stay in touch with relatives and friends and communicate with business associates. It is often difficult to recognize whether an e-Mail is legitimate. Scammers who use e-Mail for online fraud are adopting increasingly sophisticated Social Engineering techniques for duping consumers, including the use of images and logos that appear to be from the legitimate company. Play it safe when using e-Mail by following these simple tips:

• Don't reply to any e-Mail requesting personal information: Bank-Fund Staff Federal Credit Union, like most legitimate organizations will not send you unsolicited e-Mails requesting that you reply with information considered personal or private, such as:

- Member Number
- ATM PIN
- OBSN
- Online Banking Password
- Credit Card Number
- Card Expiration Date
- Birthday
- Driver's License Number
- Mother's Maiden Name

• Never send e-Mail containing confidential information: e-Mail is not a secure method for sending private information and is typically not encrypted or encoded in any form.

• Avoid e-Mails from unknown senders: If you don't know the sender, delete it. It is possible for e-Mails to contain Viruses, Trojans, or other malicious software that may cause damage to your computer. Other e-Mail may contain links to websites hosting malicious software or attempts to "fish" for live e-Mail addresses; do not reply or click on links where prompted to "unsubscribe" from a list, in a vast majority of these cases they simply confirm that you e-Mail address is valid and is then sold to Spammers, increasing the amount of unsolicited e-Mails.

• Be wary of offers or requests: Offers for free products, money, or gifts requesting personal information are typically not genuine. If an e-Mail sounds too good to be true, it probably is; delete it.

• Type, don't click: Some links within e-Mail will redirect you a phony look-alike site that will prompt you for confidential information, such as Online Banking authentication information; verify that the web site linked off of an e-Mail is legitimate before providing any confidential information. Other links may direct you to sites containing malicious software or validate your e-Mail address to a Spammer, who will in turn sell it. Always type the link in the e-Mail in the browser instead of clicking on the link in the e-Mail as the link may not redirect you to the web site it indicates.

• The following are common characteristics of fraudulent e-Mails:

- Urgent tone: Fraudulent e-Mails typically contain language stating that a failure to verify personal information will result in a suspension, termination of account access or legal action.
- Arrive unsolicited: While the vast majority of unsolicited e-Mails are usually simply annoying junk or spam, a certain percentage will typically contain Phishing or more insidious attacks.
- Forge a sender's e-Mail addresses: The fraudulent e-Mail will typically disguise sender's e-Mail address so it appears to have originated from a legitimate organization.

## How do I know the e-Mail I received is from BFSFCU?

Fraudulent e-Mails may contain logo and images from Bank-Fund Staff Federal Credit Union web site or even appear to have originated from a legitimate BFSFCU e-Mail address. The important thing to note is that Bank-Fund Staff Federal Credit Union will never send you unsolicited e-Mails requesting personal information. If in doubt, please contact us directly before responding to any such e-Mail or to report suspect fraudulent e-Mails.

## How did a spammer get my e-mail address?

Spammers can obtain or purchase e-Mail lists through both legitimate and illegitimate sources or randomly generate e-Mail address lists using computers. Spammers may also "fish" for valid e-Mail addresses using fraudulent e-Mails that appear to be from legitimate organizations and request that you "unsubscribe" from their mailing lists. We assure you that your e-Mail address is highly protected at Bank-Fund Staff Federal Credit Union. We do not purchase, sell, or trade personal or account information – including e-Mail addresses.

## How can I prevent these fraudulent e-Mails?

Many e-Mail applications and services now have spam filters that minimize the amount of spam you receive. These filters can help to minimize the amount of fraudulent e-Mails you receive. Keeping anti-spam, anti-virus, and anti-spyware software installed and up to date on your computer makes it more difficult for scammers to access your personal or financial information. Such third party software is readily available from all major retail stores or via the Internet.

## How do I report a suspicious or fraudulent e-Mail or web site?

If you suspect you may have received a fraudulent e-Mail or link to a fraudulent web site, please forward it and information regarding the e-Mail or web site to websecure@bfsfcu.org. This e-Mail address is intended for the sole purpose of handling suspected fraudulent e-Mails and web sites.

If you believe you have provided personal or account information in response to a fraudulent e-Mail or web site, please contact a Bank-Fund Staff Federal Credit Union representative immediately by calling us at 1-800-923-7328 and request to have an alert placed on your account. Please be sure to forward any relevant information regarding the fraudulent e-Mail including e-Mail address, subject, and the names of any attachments.

## Has BFSFCU been the target of online fraud?

Many financial institutions and companies that conduct business on the Internet, including Bank-Fund Staff Federal Credit Union, have become the target of online fraud in the form of Phishing, Pharming, and Social Engineering. We're aware of online fraudulent activities and have aggressive policies in place to fight online fraud. We have a team dedicated to online fraud and we are working with law enforcement agencies, industry groups, and other financial institutions to help minimize the impact of online fraud. We're also proactively communicating with our members and employees to help educate them about online fraud.

## How can I protect myself from online fraud?

With proper precautions and vigilance, you can protect your personal and financial information:

- Keep your computer operating system and Internet Browser current with the latest security patches or upgrades.
- Maintain anti-virus, anti-spyware, pop-up blocker, and anti-spam filters current and up to date; run routine scans against your computer to verify the security of your own system.
- Avoid downloading and / or installing programs from unknown sources
- Use strong passwords, cycled regularly
- Watch out for phony look-alike sites
- Don’t respond to unsolicited requests for personal or account information
- Only submit personal information via secure web sites you have verified are legitimate
- Do business only with companies you know and trust
- Keep your personal information in a safe and secure place
- Report lost or stolen credit cards, driver’s license, Social Security cards, ATM cards, and passports immediately
- Leave out personal information on your checks
- Review your financial statements regularly
- Dispose of confidential information in a safe and secure manner including canceled or unused cards and checks
- Review your Credit Reports on a regular basis

Please refer to the section “What You Can Do” for more information.

## How is BFSFCU protecting its members from online fraud?

The security of our members’ accounts and personal information is our highest priority. We have a team dedicated to member security and fraud investigation and we are working with law enforcement agencies, industry groups, and other financial institutions to help minimize the impact of online fraud. We have aggressive processes, policies and technologies in place to help us fight these scams. We're also proactively communicating with our employees and our clients about online fraud.

## Should I be concerned about someone stealing my identity?

Identity Theft is a very real and dangerous threat that may take a relatively long time before it is discovered by the victims. Bank-Fund Staff Federal Credit Union takes this threat and the protection of the confidential information entrusted to us very seriously. You can learn more about Identity Theft and what you can do to protect yourself through our Identity Threat Homepage.

## How can I protect myself from Identity Theft?

With proper precautions and vigilance, you can protect your personal and financial information:

- Keep your computer operating system and Internet Browser current with the latest security patches and / or upgrades.
- Maintain Anti-virus, Anti-Spyware, Pop-up blocker, and Anti-Spam filters current and up to date; run routine scans against your computer to verify the security of your own system.
- Avoid downloading and / or installing programs from unknown sources
- Use strong passwords, cycled regularly
- Watch out for phony look-alike sites
- Don’t respond to unsolicited requests for personal or account information
- Only submit personal information via secure web sites you have verified are legitimate
- Do business only with companies you know and trust
- Keep your personal information in a safe and secure place
- Report lost or stolen credit cards, driver’s license, Social Security cards, ATM cards, and passports immediately
- Leave out personal information on your checks
- Review your financial statements regularly

- Dispose of confidential information in a safe and secure manner including canceled or unused cards and checks
- Review your Credit Reports on a regular basis

Please refer to the section “What You Can Do“ for more information.

## What are some signs that I may be a victim of Identity Theft?

Identity Theft can be dangerous because it may remain hidden for a relatively long period of time before it is discovered. Here are some possible signs that you may be a target or victim of Identity Theft:

- Missing mail: If you begin to notice mail is missing, in particular regular banking statements or bills
- Suspicious transactions: If you notice unusual activity on your Bank-Fund Staff Federal Credit Union account(s), credit card bills, or Credit Reports.
- Unexpected credit refusals: If you are suddenly unable to obtain a loan or mortgage despite a record of good credit history
- Unusual calls: Calls from businesses, financial institutions, credit card companies or collection agencies regarding merchandise or services you do not recognize
- New credit cards or bills: You receive a new credit card or bill in the mail for a service or loan you did not apply for

## What to do if I am a victim of Identitiy Theft?

If you suspect that you’re a victim of online fraud or identity theft, follow these steps immediately:

- Notify one of the three major credit bureaus and place a fraud alert on your credit report. Call the toll-free number of any of the three major credit bureaus to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. Once the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified.
- Contact your financial institutions and credit card companies. Close the affected accounts and open new ones with new personal identification numbers and passwords.
- Contact the local police department and ask to file a miscellaneous incident report. Even if the police do not catch the criminal, having a police report can help you clear up your credit records.
- Ask for the case number and copy of the report.
- Contact all the businesses that have opened accounts in your name without your permission. Close the accounts and let the businesses know that the accounts were opened fraudulently. Make sure you communicate with the businesses in writing.
- Notify the Federal Trade Commission. Call 1-877-ID-THEFT (438-4338) or visit www.consumer.gov/idtheft. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials track down identity thieves.
- Report stolen mail. File a report with the Postal Service. Call your local Postal Inspector or visit www.usps.com.
- Call the Social Security Fraud Hotline. Immediately report that your card has been lost or stolen by calling the Hotline at 1-800-269-0271.
- Report stolen checks. If your checks have been stolen or misused, request stop payments for all affected check numbers.
- Please forward any fraudulent or suspicious e-Mails or websites to websecure@bfsfcu.org to assist us in preventing further members from being victimized.