DISCOVERY

A Quarterly Newsletter - October 2017

Equifax Data Breach - Helpful Tips

On September 7, 2017, Equifax reported a data breach, responsible for the loss of personally identifiable information/data of over 145.5 million consumers. This very likely means that you or someone in your immediate family is likely to be impacted by the loss of this personal data.

The breach, which was initially discovered in July 2017, included the loss of first and last names, Social Security numbers, birth dates, addresses, and in some cases, driver's license information. An additional loss of 290,000 credit card numbers was announced by the Equifax breach disclosure team.

You can visit the Equifax Cybersecurity Incident response website at the following website:

https://www.equifaxsecurity2017.com

At the site, you can enter a minimum of information to help identify whether you or a family member may have been part of the data breach.

Here are a few suggestions to protect your credit report and potentially prevent identity theft.

1. Monitor your credit reports for unusual/unauthorized activities.
2. If you don't need a loan in the short term, you can lock your credit report. Do so at all three bureaus (Equifax, Transunion, & Experian).
3. You can also put a fraud alert on your report at all three bureaus as well, but this can make getting a loan more difficult in the short term.
4. Enroll in a credit report monitoring and identity theft protection program like ID*Protect, LifeLock, or TrustedID Premier.
5. Be extra suspicious of unsolicited emails, if in doubt - THROW IT OUT! (Delete it!)

RATES

Money Markets

Basic	$500 - $10,000	0.45%
Bronze	$10,001 - $50,000	0.47%
Silver	$50,001 - $100,000	0.50%
Gold	$100,001 - $150,000	0.53%
Platinum	$150,000+	0.55%
Regular Share		0.20%
Variable IRA		0.40%

*** Rates subject to change without notice**

In this issue:

*ID*PROTECT IS AVAILABLE!*

Protect Yourself Online
For member/owners who are concerned about the Equifax Data Breach or if you're worried about future breaches, now is the perfect time to enroll in ID*Protect.

With ID*Protect, Quest Federal Credit Union's identity theft protection partner, ID*Protect gives you everything you need to safeguard your identity, protect your credit and help you recover should you become a victim of identity fraud. ID*Protect can be added for your protection at any time, it costs just $4.00/month if you do not have a current loan with Quest Federal Credit Union, for members with current loans, the monthly fee is waived for the life of the loan.

For more information, go to:
https://questfcu.com/member-services/idprotect/

With ID*Protect's Resolution Services
Should you become a victim of identity theft, ID*Protect provides you with access to a case manager who provides end-to-end recovery support on your behalf. Working as your advocate, the case manager handles everything from reviewing your credit report with you to notifying relevant agencies and creditors. They will assist you in placing fraud alerts on your credit report and will create your personal case file. Your case manager is there to walk you through the entire recovery process – until your identity and credit are completely restored.

Protect Your Family - Including Your Children
Not only does ID*Protect safeguard the head of the household, it also protects ALL members of your household, including your children. While your children may not have any credit history, it is possible for ID thieves to obtain and utilize the personally identifiable information for anyone who has a name, birth date, and Social Security number. Using this information, ID thieves can open credit lines in your children's names and ruin their credit well before they might need it for a car, credit card, or student loan.

For more information, go to:
https://questfcu.com/member-services/idprotect/

OCTOBER is Cybersecurity Awareness Month

October is National Cybersecurity Awareness Month. During the month of October, Quest Federal Credit Union is promoting various cybersecurity topics to ensure that our member/owners and their families & friends are aware of common cybersecurity topics and threats to your online safety.

Common Threats

Below is a small list of everyday, common tactics used to steal, scam, and harm individuals who are online and connected.

- **PHISHING** - PHISHING is the term used when bad actors send unsolicited email (junk) with requests for information, malware, and viruses intended to collect personal and financial information. Cybercriminals attempt to trick users into clicking a link or file attachment that cause a vulnerability. Phishing emails often look like an email from a legitimate online source, like shopping, gaming, government, or financial institutions. Phishing emails often contain language that intend to confuse or threaten action and an immediate need to respond.
- **MALWARE** - Malicious software, or MALWARE for short, is software intended to exploit a vulnerability or create a vulbnerability on your computer that is in turn used to capture or steal your personal and/or financial information. Adware, Botnets, Spyware, Virus, Trojan, Ransomware, & Rootkit are all terms for types of MALWARE responsible for exploiting and stealing information from users.
- **RANSOMWARE** - A special type of malware, RANSOMWARE, has gained in popularity in the last few years. Ransomware is a kind of malware that is installed on your computer and systematically encrypts and locks all of the files on your computer. Once the files are encrypted and locked, they can only be unlocked by paying the criminals a ransom. If the ransom is paid, typically the unlock code is transmitted and the files are unlocked and made usable again.
- **UNSECURED PUBLIC WI-FI** - Never connect to an unsecured wireless network that you are not familiar with. Once connected to an unsecured wireless network, bad actors can see all online activity and capture transmitted information, especially information used to access secured sites, such as email, social media, and most importantly, online financial account information - credit union access, bank access, credit card company access, etc.

These are just a few threats, but are very common and can easily be protected against with some very manageable tactics to prevent and deny unauthorized access to your computer, mobile devices, and other Internet-connected devices.

Common Protections

Put some of these protections into use and you can protect yourself and your family from becoming another victim.

- **Think before you connect!** Before you connect to that wireless network, confirm the name of the network or login process from appropriate staff. Cybercriminals can easily create wireless networks that are similarly named and allow for the theft of your personal information.
- **When in doubt, throw it out!** Links in email and online posts should be reviewed, if it looks suspicious or if you don't recognize the source, mark it as "junk" or delete it immediately.
- **Think before you act!** Be wary of communications that intimidate, threaten, or implore you to act immediately. Additionally, if the offer sounds too good to be true, it probably is! Delete that email.
- **Make passwords strong, long, and difficult to remember!** It may sound contradictory to make a password something difficult to remember or long. However, in doing so, you can make it more difficult for a cybercriminal to break your password or impossible to guess. Use a password manager to securely store and randomize all passwords. Never use the same password twice!!!
- **Use Multifactor Authentication!** When it is available, use multifactor authentication, such as a PIN delivered via SMS text message or other one-time system to gain access to your mobile banking, credit card account, email account, or social media account.
- **Keep your systems updated!** Change can be difficult, but in recent years, updates to your computer operating system, mobile phone, and tablet have been less disruptive. Always update your computer and mobile device, this is how Microsoft, Apple, Google, and others patch and help you guard against vulnerabilities that have been found.
- **Back up your system(s)!** By regularly backing up your computer or mobile device, you minimize the risk of complete system failure and you will also be able to restore data should you fall victim to a ransomware or other malware attack!

Download the QUEST FCU mobile app today for your Android and Apple devices to take advantage of complete account access while on-the-go!

Member./owners can download the app from your app store and gain immediate access to your on-line account as well as transfer money, pay bills, review transactions, and now --- perform mobile deposits from anywhere!

Mobile deposits require registration and an account in good standing, generally speaking, most members will qualify for mobile deposit. Registration requests are handled daily and the process is quick and easy. For more information, go to:

https://questfcu.com/rdc/

Holiday Season - Almost!

The holidays are almost upon us, which is hard to believe! We would like to take a moment to remind members to review our upcoming holiday schedule.

- October 9 - Columbus Day
  All offices closed
- November 23 - Thanksgiving Day
  All offices closed
- December 25 - Christmas Day
  All offices closed
- January 1 - New Year's Day
  All offices closed

Call for Candidates!!!

Quest Federal Credit Union will hold its Annual Meeting on March 17th, 2018 at the Plaza Inn of Mt. Victory, OH at 9:00 am. Any eligible voting member interested in petitioning for inclusion on the 2018 Ballot for Board of Directors or Credit Committee may request a petition packet in writing by contacting the Nominating Committee Chair in writing, no later than November 17, 2017. All petition packets must be returned in its entirety to the Nominating Committee Chair no later than December 18, 2017.

Quest Federal Credit Union
Attn: Nominating Committee Chair
12837 US Highway 68
Kenton, OH 43326

ADDENDUM – Call For Candidates: Let this addendum serve as notice that per the bylaws of the Quest Federal Credit Union, if there is only one nomination for each board position opening and no candidate by petition, it will be determined that there is no contest by the Nominating and Supervisory Committee and no ballot will be mailed. Thank you, Quest Federal Credit Union

Quest™
Federal Credit Union
Explore the Possibilities

LOCATIONS: **www.questfcu.com**

Kenton:	**12837 US 68 South**	**(419) 674-4998**
	101 Jacob Parrot Blvd.	**(419) 675-2322**
Ada:	**232 N. Main St.**	**(419) 634-0031**
Bellefontaine:	**900 East Sandusky St.**	**(937) 599-1321**
Upper Sandusky:	**1725 E. Wyandot Ave.**	**(419) 835-1101**

EQUAL OPPORTUNITY LENDER

NCUA