

# **WARNING**

## **DUE TO THE RECENT EQUIFAX BREACH...**

Equifax, a major consumer credit reporting agency, was hacked from mid-May to July. Approximately 143 million American consumers have been or will be affected. The possible information that was stolen from this company includes the following:

- Social Security numbers
- Some Driver's license numbers
- Names
- Birth dates
- Addresses
- 209,000 Credit card numbers
- 182,000 Documents with personal information used in disputes

An FBI spokesperson has stated that the agency is aware of the breach and is currently tracking the situation.

In light of this breach and the sensitive information stolen, Indianhead Credit Union will be asking that you have a keyword/number placed on your account to use as security when calling for information. Be sure to pick a keyword/number that you will remember. We will no longer be asking for the last four of your social security or date of birth to verify your identity. Please make sure when picking a keyword/number you choose something not found on social media or something easily obtained. If you have more than one account this keyword/number will be used for all accounts.



# HELPFUL TIPS TO CATCH FRAUD



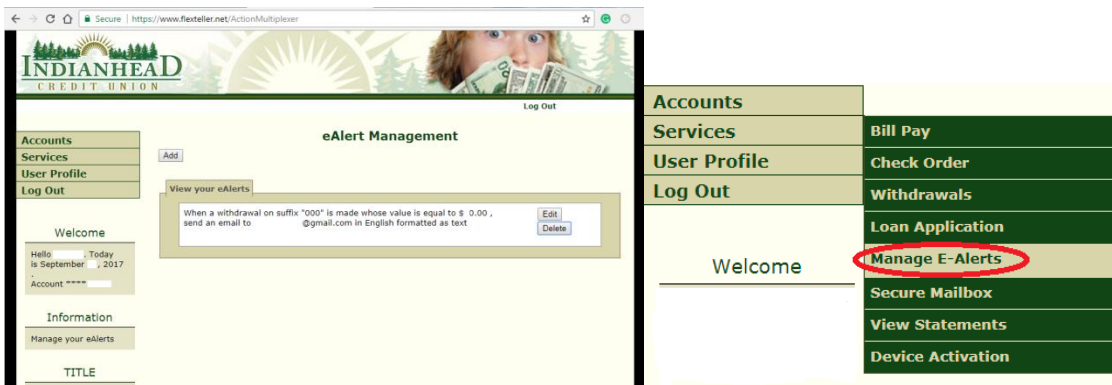
## MONITOR YOUR ACCOUNT

Monitoring your account is your best defense. You need to review your account on at least a monthly basis via your statements or online. If you have online access you can monitor your account on a daily basis. If you don't have online access; you can call our automated phone system (HAL) to monitor your account daily.

## E-Alerts

E-Alerts is a service we offer that will send you e-mails or texts letting you know about transactions on your account. You can set up alerts for when your current balance changes or goes below a certain dollar amount. You can also set up alerts for deposits, withdrawals, or checks clearing.

To set up ICU e-alerts, log into your ICU account via the website. On the left side there is an option to go to Services, under this option is Manage E-Alerts, from there you can add/manage your e-alerts.



## My Mobile Money

My Mobile Money is a way to control your debit cards transactions from your mobile device. You can set up controls (denials of certain transactions) or alerts (text messages) on all your card transactions. You can set up controls or alerts by location, merchants, transaction types or dollar limits. This app helps you monitor where your debit card transactions are allowed.

To get set up with My Mobile Money:

Visit iTunes or Google Play and search for "My Mobile Money Access"

- Click the sign up free button
- Enter your card number, enter your CVV (the three-digit number on the back of your card) and your expiration date.
- After you accept the app Terms and Conditions and the Privacy Policy, you will be asked for your email address, user name and password.

## Phishing Scams

A Phishing Scam can be a call or e-mail; this is when someone calls or emails pretending to be a legitimate company. Unless you have called the company yourself, do not give out personal information.

## Checking Your Mail

Please make sure you are opening all your mail. What normally may look like an advertisement or a credit card offer might be a fraudulent bill.