FEDERAL CREDIT UNION
1-800-634-9239 - www.acmgfcu.org

Identity Theft Guidelines

What to do:
Determine what information was stolen or compromised.

1. If debit or credit card data was compromised, your card can be blocked and a new card issued to prevent thieves from accessing money in your ACMG account or making credit card purchases.
2. If your credit union account numbers were compromised (stolen checkbook, account paperwork etc.), we can perform an account sweep to provide you with new account numbers. This would prevent fraud on your original account. Members with our checking account will be assigned an Identity Theft Recovery Advocate to help you through the process of monitoring your credit and replacing stolen identification.
3. If data is stolen that includes social security numbers, birth date, medical or other highly sensitive personal information, we recommend you consider the steps below to protect your identity and carefully monitor for signs of potential use of your information.

Steps You Can Take to Protect Your Identity:

When you make a payment on a credit card or loan, the business that gave you the loan keeps a record of how much and often you pay, as well as the credit limits and loan balances. That information is sent to one or more credit reporting companies. The credit reporting companies (Experian, Equifax, and TransUnion) compile that information into a report and assign you a credit score. You are entitled by law to one free report per year from each of the three companies.

- Many fraud prevention experts recommend requesting your credit report from one of the three credit reporting companies every 4 months. This will allow you a free way to monitor your credit activity over the course of a year. You can place this request at https://www.annualcreditreport.com or by calling 1-877-322-8228.
- Consider filing your tax return as soon as possible each year. Identity thieves could use personal information to file fraudulent tax returns to obtain the refund you may be owed..
- Watch your mailbox or email for unusual notices. If you are unsure about something you've received, please bring it to our attention. NEVER respond to any type of request for account login information or share personally identifying information if there is not a legitimate reason for the request.
- If highly sensitive personal information was stolen, we recommend you place a fraud alert by visiting one of the three credit reporting company websites and selecting Place Fraud Alert. This 90 day fraud alert will only need to be placed at one of the agencies, they will automatically notify the other two. If you have created an Identity Theft Report, you can place an extended fraud alert on your credit file which stays effective for 7 years.

The credit reporting agency websites are:

TransUnion	https://www.transunion.com/
Experian	https://www.experian.com
Equifax	https://www.equifax.com/

Available ACMG Fraud Solutions:

- Identity Fraud Recovery Services – All ACMG members with a checking account have identity fraud recovery services in the event your personal information is used without your permission. Visit our Fraud Solutions page at https://www.acmgfcu.org/resources/learning-center/fraud-solutions to read more about the steps our Recovery Advocates provide you. If you do not have an ACMG checking account and want recovery services, you can purchase individual or family coverage with special member-only pricing from our trusted partner.
- If you want to add monitoring of your credit, additional Identity Fraud Monitoring Services can be purchased at member-only discount rates. Fraud recovery and fraud monitoring information can be viewed at https://acmgfcu.merchantsinfo.com/fully-managed-recovery.aspx
- Purchase Alerts – Visa Debit and Credit Cardholders can sign up to receive no-cost alerts on usage of their debit and/or credit cards to help monitor for fraudulent activity. To sign up for real-time alerts, visit https://usa.visa.com/pay-with-visa/featured-technologies/purchase-alerts.html and enroll all your VISA cards.
- Online Banking and our Mobile App can be used to monitor your credit union account for unauthorized activity. Login at least weekly to review your transactions or setup no-cost eAlerts that notify you of purchases and withdrawals. Consider enrolling in eStatements so you'll have the ability to view your monthly account statement more quickly and our online Bill Pay can reduce the chance of paper check fraud by sending more of your payments electronically.

What to do if your information was used:
If your personal information was used without your knowledge to obtain a loan or credit in your name, contact ACMG to report the theft immediately. Members with our checking account have full identity fraud recovery services.

- ACMG staff will make a call to the Identity Theft Recovery service and you will be assigned a Recovery Advocate to help you through the process of restoring your credit. Your advocate will complete a full Identity Fraud Threat Assessment, review all 3 credit reports for new or suspicious activity, assist with placing fraud alerts, perform research to uncover any additional fraud, create and maintain a law enforcement grade case file to assist law enforcement in the prosecution of perpetrators, activate credit monitoring during recovery, and provide your Credit Report and Score.

Learn more:
If you want to learn more about steps that can be taken to report identity theft and to obtain a recovery plan, visit the Federal Trade Commission's (FTC) website at https://www.identitytheft.gov/. The FTC's website also provides information on identity theft prevention and current scam information to help keep you informed.

acmg
FEDERAL CREDIT UNION

315-488-4433 or 1-800-634-9239

Effective: 9/18/17