ECU Identity Theft and Fraud FAQ

What is identity theft?

Identity theft can be defined as an illegal use of an individual's personal information, such as a Social Security Number, to establish new accounts or new loans. It can also include fraud committed against your current Eastman Credit Union accounts, such as ACH or share draft forgeries. No matter how you define it, identity theft is not pleasant to deal with, if or when it happens to you. ECU is here to help you if it does, and we have some suggestions to help you prevent it from happening. Here they are...

Info to help avoid becoming a victim of identity theft:

Carry only those pieces of identification you absolutely need.

Make a photocopy of the contents of your wallet and store them in a safe place.

Shred any documents containing financial or personal information before throwing them away.

Do not give personal or account information to anyone over the phone.

Only use secure websites when shopping online or surfing the web.

Store all checks (new and canceled) in a safe place.

Don't include your Social Security number or driver's license number on your checks.

Review monthly accounts and credit card statements for unauthorized charges.

Report any lost or stolen checks, credit and debit cards immediately.

What is the difference between identity theft and account fraud?

Identity theft can happen when someone obtains your personal information, and then attempts to acquire loans or other accounts in your name and/or Social Security number. Account fraud is when someone steals your checkbook and then writes checks to themselves or others, but does not attempt to assume your identity. It's not unusual for identity theft to lead to other types of fraud, so in some instances the two may go hand in hand. ECU is here to help you navigate through the process of identifying when you are the victim of identity theft and/or account fraud.

My identity was stolen. What should I do?

This can seem like an overwhelming situation but with a little time and effort, you can get it all back under control. We put together an Identity Theft Info Sheet at the bottom of this FAQ that will help you get things back on track.

What if the identity theft involves my ECU accounts?

We're here to help! Contact ECU immediately at 1-800-999-2328. You may also visit any ECU branch location and work with a Member Service Representative to take additional steps to protect your identity. You should also review the Identity Theft Info Sheet at the bottom of this FAQ for additional steps you can take when your identity is stolen. We will be glad to help guide you through this process.

I think my identity was stolen online. What do I need to do?

First things first. Turn off any device you think is compromised, and immediately reset ALL of your passwords for email, social media, shopping, banking, etc. from a different computer/device than the one you believe is compromised. ECU also recommends that you have your computer/device professionally inspected and cleaned prior to allowing you to access ECU Online again. We will take steps to protect your ECU Online account access, including blocking all access to it until you notify us that your computer/device has been cleaned. In addition to blocking ECU Online access, we will also need to close and reopen new accounts for you. We do this because your account numbers could have been compromised and used at any time. That's not something you want to deal with down the road, it takes a little time but it's well worth it when this happens.

I didn't allow anyone to use my computer/device, but I have given someone my ECU Online login credentials. What should I do?

Change your ECU Online user ID and password now! Seriously, stop reading this and do it, you can pick this back up in a minute. Contact ECU at 1-800-999-2328 if you don't know how to change your ECU Online user ID and password and we'll be glad to help. We also need to close and reopen new accounts since your account numbers may have been compromised. NEVER give anyone your ECU Online login credentials.

What should I do if I notice an unusual transaction on my account?

Contact ECU immediately. We will work with you to determine more about the transaction and take appropriate action. There are time constraints on certain types of transactions so it's imperative that you review your accounts on a regular basis and notify us immediately if you notice something unusual. Reviewing your accounts regularly is one of the best proactive things you can do!

What if my personal information was physically stolen? This may include your purse, wallet, phone, mail, and even your trash.

You should file a police report as soon as possible. Contact ECU if any of the information was related to your ECU accounts. Depending on the information that was taken, we will advise you on steps you can take to protect your identity. If your phone is stolen, you should also contact your service provider and have the phone blocked. They might also be able to remotely wipe the device, to help prevent additional information theft. Smartphones contain a large amount of data about you, and if someone is able to access the phone, it may give them access to additional personal information that they could use. Refer to the Identity Theft Info Sheet at the bottom of this FAQ for additional steps you can take in this situation.

If I discover a loan or deposit account I don't recognize, what should I do?

Contact the institution where the account or loan is established. Request more information to determine if the account is legitimate or if it was opened fraudulently. If you determine that it is fraud, file a dispute with the institution. You can also refer to the Identity Theft Info Sheet at the bottom of this FAQ for some additional steps you can take, in addition to filing a dispute.

What if the deposit account or loan I don't recognize is with ECU?

Contact ECU immediately at 1-800-999-2328. We hate ID Theft and Fraud just as much as you do! We will investigate the account and let you know what we find. We will take the appropriate actions, and please know, that if it's not your account or loan, you will not be held responsible for it.

I reviewed my credit reports and I found an account that I didn't open. What do I do now?

If the accounts are with ECU, please contact us immediately at 1-800-999-2328 and we will investigate them and let you know what action needs to be taken. If the accounts are with another institution, contact that institution and ask for additional information on the accounts. If you determine that the accounts are fraudulent, refer to the Identity Theft Info Sheet at the bottom of this FAQ for additional steps you can take.

What if I think someone I know or a family member is trying to access my information?

Contact ECU if you believe this is occurring on your accounts with ECU. We will work with you to protect your accounts.

I am concerned about the Equifax Credit Bureau breach and data breaches in general. What can I do to protect my identity?

We understand, and you should be concerned. Here are some things you can do to protect your identity now and in the future:

> Equifax has provided a website for consumers to obtain updated information and to determine if they have been impacted by this breach. That website is: www.equifaxsecurity2017.com
>
> Equifax will provide a year of free credit monitoring to consumers. They can request this service at the Equifax site mentioned above.
>
> Check credit reports. Consumers can obtain these for free at www.annualcreditreport.com. It may be prudent to order a credit report from a different agency every few months instead of ordering credit reports from all agencies at once.
>
> Monitor all credit card and online accounts closely for unauthorized activity
>
> Consider placing a credit freeze on credit reports. This will make it difficult for someone to open credit accounts under your name. For more information about a credit freeze, visit the Federal Trade Commission website at consumer.ftc.gov
>
> File taxes as early as possible. One common form of identity theft happens when someone with access to your SSN files taxes under your name before you do in order to obtain tax refunds.
>
> Consider opting out of offers for new credit and insurance that are sent via postal mail. Identity thieves like to intercept these credit offers and open lines of credit or obtain insurance fraudulently. To opt out, consumers can call 1-888-567-8688 or visit www.optoutprescreen.com

ID Theft Info Sheet

Make a list of all the accounts, cards, loans, etc. that you know you have. This will be useful as you work through the process of recovering your identity.

Notify local law enforcement of the activity/crime. (Note: It's best to file a police report for fraudulent activity or identity theft in the district the crime occurred.)

Close other accounts if your SSN, in conjunction with your identification and/or name and address, has been compromised.

File a complaint with the Federal Trade Commission (FTC) at 1-877-438-4338 or visit the identity theft section at www.ftccomplaintassistant.gov

The 'Report Identity Theft' section of the www.ftc.gov website provides possible recovery steps.

Notify the credit bureaus in writing of the fraudulent activity and request a copy of your credit report from each credit-reporting agency. Verify the information is accurate on each one. Ask that your name be removed from mailings and that no credit be issued without calling your home phone first.

Equifax 1-888-766-0008 Fraud Hotline (www.equifax.com)

Experian 1-888-397-3742 Fraud Hotline (www.experian.com)

TransUnion 1-800-680-7289 Fraud Hotline (www.transunion.com)

Innovis 1-800-540-2505 Fraud Hotline (www.innovis.com)

Contact the US Postal Inspector at 800-275-8777. It is not uncommon for perpetrators to change your address so that they receive credit cards, bills, etc.

Contact your local DMV (Department of Motorized Vehicles) to put a hold on your driver's license to prevent anyone from having another driver's license issued in your name. You may want to request a new driver's license number.

Contact ChexSystems, Inc. at 1-800-428-9623 and request a free consumer report to determine if a new bank account has been opened in your name and social security number.

Continue to verify all account activity, reconcile monthly bank statements, debit card and ACH transactions.

Be aware of any e-mails that may result from the thief asking for additional personal or financial information. No financial institution or reputable company will ask you to send private information by email. Never assume public email is secure.

Other web sites that may be helpful in reporting scams/fraudulent activity are:

www.identitytheft.org
www.ic3.gov

EASTMAN CREDIT UNION®
ECU BESIDE YOU