KANSAS FARM BUREAU®
Legal Foundation

www.kfb.org/legalfoundation

Wendee Grady, Director
2627 KFB Plaza
Manhattan, KS 66503-8158
785.587.6101

Identity Theft and Cybersecurity

Identity theft. If it hasn't happened to you, you probably know someone impacted by it. Identity thieves use a person's information to do things like apply for a credit card or loan in their name, access their bank account or use their credit card, file a fraudulent tax return or insurance or benefit claim, or sell the information to someone else for fraudulent use.

The year 2020 saw a staggering number of unemployment claims for the State of Kansas, with 24% or more of these claims (at least $300 million worth), being fraudulent.[1] In addition to the clear monetary cost, the influx of fraudulent claims overwhelmed the Kansas Department of Labor and slowed valid claims for unemployment during the COVID-19 pandemic, when many families desperately relied on timely processing and payment of their claims. Identity theft can clearly be a burden to society, and it can be costly to individual victims.

What are some signs of identity theft?

There are many ways to identify identity theft, but some of the most common things are:

- **Household bills no longer in the mail.** This could mean someone has stolen mail that could have personal information on it, or that someone has accessed your account and changed the billing address.
- **Credit denied.** If you have good credit, but have an application for new credit denied, or approved at a higher interest rate than you expect, you might have been a victim of identity theft. It might be helpful to take a more proactive approach and monitor your credit. You can create accounts with the three credit bureaus[2] and occasionally check your credit history, including recent inquiries, to see if someone has tried to access your credit. Alternatively, there are credit monitoring services that you can purchase and let a company do that work for you.
- **Unexpected bills/charges.** If you receive a bill for something you didn't purchase, or if you have an unauthorized credit card charge or bank transaction, it can be a sign of identity theft. Look for small "test" charges, too. No kidding, I logged onto my online banking account once to see a small test charge, and the description read, "CROOKS."
- **Rejected tax return.** If you file your tax return and receive a rejection notice from the IRS due to a duplicate return, that could indicate someone else has fraudulently filed a return in your name to claim your refund.

How can identity theft be prevented?

Taking the following steps can help prevent identity theft:

- **Protect your SSN.** Don't carry your SS card with you except when necessary to conduct business (like when opening a bank account).
- **Protect your paperwork.** Don't leave your mail in the mailbox overnight or for longer periods of time, and securely store or destroy all paperwork with sensitive information on it.
- **Watch for scams.** Learn about scamming methods, such as phishing[3] and spoofing,[4] so you can identify these efforts and don't become a scammer's next victim. Double check senders of texts and emails, and examine the content in a message, before clicking on any links or attachments.
- **Passwords.** Use strong passwords and a password manager to create and store passwords that vary greatly from site to site, so that if one website is compromised, your whole digital presence isn't put at risk.
- **2-Step (Factor) Authentication.** Use a 2-step authentication when it's available. I can speak first-hand about the value of this. I woke up one morning to learn that someone had tried to access my retirement account in the middle of the night, but luckily their attempt was blocked when a 2-step authentication required them to enter the code I had received by text on my mobile phone.
- **Create your own internet presence.** Avoiding the internet won't necessarily keep your identity

safe. If you don't already have a social media presence or online accounts for services you use, it becomes even easier for a fraudster to set up an account in your name and use it for their benefit. Some good accounts to start with are: 1) the U.S. Postal Service, 2) the three credit bureaus, 3) the Social Security Administration, and 4) your banks.

- **Don't overshare on social media.** Don't join in social media exercises listing out personal information about your current relationship, family, furry friends, hobbies, etc. Those types of posts are often launched by fraudsters as a data harvesting effort to collect information from unsuspecting social media consumers. Much of that information can be used to hack passwords or security questions used to access accounts. Additionally, check your social media and other app security and privacy settings regularly to make sure that you haven't granted those providers and companies access to too much of your personal account information, and that their standard security and privacy settings haven't changed since you established your account.

What should be done after identity theft?

Whether it is a fraudulent unemployment claim, or other form of identity theft, there are some basic steps to be taken to prevent further cost and impact from theft.

- Review your credit report with one or more of the credit bureaus to check it for inaccuracies.
- Place a credit freeze on your account with the credit bureaus, or at least place a 1-year fraud alert on your accounts, which requires potential creditors to verify your identity before issuing new credit.
- Contact your banking institutions and credit card companies, and consider closing any accounts that could be impacted.
- File a complaint with your local law enforcement agency. Additionally, the Kansas Attorney General Consumer Protection Division also has an online identity theft complaint form.[5]
- The Federal Trade Commission has a website that can help users report identity theft and get a recovery plan.[6]
- File your tax return early to prevent any delays caused by someone else filing your return first, in order to claim any refund you are due.

Additional steps might be necessary for particular kinds of identify theft. For example, a fraudulent unemployment claim could result in inaccurate earnings reported to the IRS or Social Security Administration and would require additional reporting to those agencies.

What resources are available to victims of identity theft?

The FTC has developed a useful guide for attorneys assisting identity theft victims, that can be helpful to attorneys and victims, alike.[7]

Finally, there are several identity protection services available for purchase before a theft has occurred. Not all services are created equal, though, and they can vary greatly in price. Services include such things as credit monitoring with the credit bureaus, identity theft insurance (commonly covering up to $1M in losses), and dark web monitoring to see if your personal information is being marketed and sold to fraudsters.

---

[1] https://www.kansas.com/news/politics-government/article249466660.html

[2] Equifax, www.equifax.com; Experian, www.experian.com; TransUnion, www.transunion.com.

[3] To learn more about phishing, and how to recognize and avoid it, visit: https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/phishing-scams.

[4] To learn more about spoofing, and how to recognize and avoid it, visit: https://www.fcc.gov/spoofing.

[5] The AG's identity theft resources, including the online complaint form, can be found here: https://ag.ks.gov/in-your-corner-kansas/your-identity/what-is-identity-theft-.

[6] The FTC's website for reporting identity theft and getting a recovery plan can be found here: www.identitytheft.gov.

[7] FTC's Guide for Assisting Identity Theft Victims: https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.