CONSIDER THIS:  

Identity Theft Is the Rise

Consumers, Be Wary:

Identity Theft Isn’t Going Away

If you’ve been a victim of identity theft, you’re not alone. In 2016’s end-of-year survey conducted by Georgia Credit Union Affiliates, 44 percent of respondents reported that they’ve been victimized by fraud and/or identity theft. More could have suffered at the hands of fraudsters without knowing it yet.

The Georgia Department of Law Consumer Protection Unit notes that in 2015 Georgia had the seventh greatest number of identity theft related complaints filed with the Federal Trade Commission. Antisecurity activities by the Federal Trade Commission, EMV cards, and new counterfeit card technologies have caused a decline in the use of counterfeit cards.

According to a study by Barclays, most credit card fraud that occurs happens in the United States (about 47 percent); 55 percent of these data breaches or identity thefts are caused by a malicious outsider, followed by an accidental loss of the card (25 percent). EMV chips (which stands for Europay, Mastercard and Visa and is a global standard to authenticate and secure global card transactions) have caused a decline in the use of counterfeit cards. These days, 45 percent of fraud is committed online.

Online fraud gives hackers and predators a multitude of ways to get your information. From creating fake forms to posing as legitimate companies, the internet has spawned a wide array of tactics to get your personal and financial information, which means consumers need to remain vigilant.

Some of the most common forms of identity theft are:

- **Child ID theft** - Children’s IDs are vulnerable because the thief may go undetected for many years. By the time they are adults, the damage has already been done to their identities.
- **Tax ID theft** - A thief uses your Social Security number to falsely file tax returns with the Internal Revenue Service or state government.
- **Medical ID theft** - This form of ID theft happens when someone steals your personal information, such as your Medicare ID or health insurance member number, to get medical services or to issue fraudulent billing to your health insurance provider.
- **Senior ID theft** - ID theft schemes that target seniors. Seniors are vulnerable to ID theft because they are more frequent contact with medical professionals who get their medical insurance information, or caregivers and staff at long-term care facilities who have access to personal information or financial documents.
- **Social ID theft** - A thief uses your name, photos, and other personal information to create a phony account on a social media platform.

Despite the prevalence of identity theft, only half of the survey respondents closely monitor their accounts to check for fraudulent transactions. On the other hand, 10 percent of respondents figure that someone will let them know if any of their accounts have been compromised and they just leave protecting their identity and accounts to their financial institutions.

Insider’s Perspective:

“IT’s important for us, as credit unions, to inject appropriate steps into our processes to protect our members from people who would do them harm,” said Allen Upchurch, President and CEO of Credit Union of Atlanta. “It’s also important for us, as an industry, to keep educating our members about how to prevent the potential threat of their key information, and about taking appropriate steps to guard against letting their names, addresses, Social Security numbers, credit union account numbers get into the wrong hands.”

Upchurch said at his credit union, staff is trained to watch out for members conducting transactions that may not be in their best interests, and proactively talk with members about protecting their assets. Many credit unions, including Credit Union of Atlanta, provide a service that should members become victims, helps them restore their identity by placing necessary alerts in their credit files, lodging disputes, coordinating with government agencies, other financial institutions and creditors to help resolve incidents, and even working with law enforcement agencies to help arrest and prosecute criminals.

“We talk to our members about the various scams that are being conducted every day, and how not to fall victim to someone they’ve never heard from before wanting to obtain information from them, or to entice them into some ‘too good to be true’ offer,” Upchurch explained. “Above all, we tell them what they can expect from our credit union in terms of any communication we have with them. For example, we will never call a member asking them to verify their Social Security numbers or other identifying information, such as their debit card PINs. It’s important that we constantly keep this subject in front of our members and staff, and to keep talking to each other about new scams and other criminal activities that abound.”

Identity theft isn’t going away, and Upchurch said everyone – consumers, financial institutions and merchants – must do their part to minimize the impact of fraudulent activity and the heavy costs associated with fighting it.

**Tips:**

Savvy consumers will take steps to protect themselves from identity theft:

- **Guard your (and your children’s) personal information** - Don’t carry your Social Security card in your wallet or write your number on your checks. Only give out your SSN when absolutely necessary. Ask if there is an alternative way for you to verify your identity. Don’t respond to unsolicited requests for personal information and store personal information in a safe place.
- **Keep an eye on your accounts** - Pay attention to billing cycles. If bills or statements are late, contact the sender. Collect mail promptly and put your mail on hold when you’re away for several days so thieves don’t have a chance to get to account information on mail left in your box. Review your receipts and compare them to your account statements. Watch for unauthorized transactions. Shred receipts and credit card offers and other paperwork you don’t need but that could contain personal information.
- **Be vigilant online** - Install firewalls and virus detection software on your home computer and create complex passwords that fraudsters can’t easily guess. Change passwords often, especially if a company or organization has your information and has suffered a database breach.
- **Order your credit report once a year** - Review it to make sure it doesn’t include accounts you have not authorized. Check it more frequently if you suspect someone has gained access to your account information.

To learn about credit unions in your community and how they can help in the event of identity theft or fraud, visit A Smarter Choice.