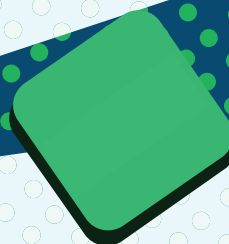


Texell

QUARTERLY

October 2026



texell
CREDIT UNION

INSIDE: ►►
Let's Talk Digital
Digital Banking Tools

WELCOME



Richard Silvers
Chief Technology Officer

Welcome to the fall 2026 issue of Texell Quarterly. As technology continues to transform the way we manage our finances, Texell remains committed to providing secure, convenient, and innovative tools to help our members bank with confidence. October is Cybersecurity Awareness Month, and this issue focuses on how technology and digital tools shape the financial industry and the important role it plays in protecting your financial well-being.

Our Digital team discusses the features and benefits of Texell's Digital Banking services, and we cover other useful financial apps for Gen Z and Gen Alpha in Let's Talk Digital. The feature story dives into the evolution of banking and how the financial industry has adapted over 250 years to keep pace with technology.

With the holidays coming up, our Scam Watch article covers how Artificial Intelligence tools are used to create sophisticated scams and offers tips to help you recognize and avoid them.

In the Meet the Team section, two professionals from the Information Technology and Software Development teams share their journey at Texell along with advice for members to keep their accounts safe.

We hope you find these articles entertaining and valuable as you navigate the ever-changing digital landscape. Thank you for your continued trust and membership. It is our privilege to serve you and help keep your financial future secure.

4 Texell Events

5 Let's Talk Digital: Financial Tools for Gen Z & Gen Alpha

7 Digital Banking Tools

8 From the Fed to Fintech The Evolution of Digital Banking



12 Beware of AI Scams During Holiday Shopping

15 Meet the Team

TEXELL EVENTS

Join us at these upcoming Texell events.

October 8 @ 6:00 p.m. – 7:00 p.m.

Medicare Education Seminar, Waco

Discover the benefits of Medicare Health Plans at our Medicare Education Seminar, Holiday Inn Express & Suites Waco South, 5701 Legend Lake Parkway, Waco, TX 76712

October 17 @ 9:00 a.m. – 10:00 a.m.

Medicare Education Seminar, Texell HQ

Join us at our seminar held in the 1948 Room at our Headquarters, 7083 Members Parkway, Temple, TX 76502.

October 27 @ 6:00 p.m. – 7:00 p.m.

Medicare Education Seminar, Texell HQ

Join us at our seminar held in the 1948 Room at our Headquarters, 7083 Members Parkway, Temple, TX 76502.

November 14 @ 9:00 a.m. – 12:00 p.m.

Shred Day: Cedar Park

Protect your identity and shred personal information and pre-approved credit offers at our Cedar Park branch, 875 W. Whitestone Blvd., Cedar Park, TX.

November 17 @ 6:00 p.m. – 7:00 p.m.

Medicare Education Seminar, Texell HQ

Join us at our seminar held in the 1948 Room at our Headquarters, 7083 Members Parkway, Temple, TX 76502.

Let's Talk Digital:

Financial Tools for Gen Z & Gen Alpha

By Kristen Reichert

Gen Z and Gen Alpha have never known a time without the internet and mobile devices, and they rely on digital tools and apps to provide seamless access, personalization, trust, and transparency. Gen Alpha, born between 2010 and 2024, benefits from parent-managed apps to pave the way for financial literacy safely and securely. Gen Z, born from 1997 to 2012, is looking for more sophisticated tools to budget and begin their investment portfolio. Let's take a closer look at popular financial apps and their features.

What financial apps are best for Gen Alpha?

For younger users, financial education begins with earning and saving money. Many family focused apps introduce financial literacy using chore tracking tied to their allowance to help children develop healthy habits early. These parent-managed apps teach money management skills and how to create savings goals. While some apps are free, premium features in the following descriptions may require a subscription.

Greenlight:

An app for parent-managed allowances tied to chore tracking. Parental controls can assign chores, automate allowance payments, set savings goals, and spending alerts.

Acorns Early:

This app also connects chores to earning, and parents and kids can track savings goals with target dates. The app also includes debit cards, and fun lessons teach financial literacy to kids and teens.

Step:

Geared toward teens, this app aims to build savings and credit with a secured credit card and Smart Pay system. Users also have opportunities to earn cash back and send and receive money from others.

(continued on next page)



What digital tools and apps work best for Gen Z?

Gen Z teens and young adults require more than basic money management. As they enter the workforce, many are looking for tech-savvy tools to track spending, budget, and begin investing.

PocketGuard:

This budgeting app provides a snapshot of disposable income by showing how much cash is on hand after paying bills and meeting budget goals. Users connect to financial accounts and can see their cash at a glance using the “Leftover” (In My Pocket) feature.

Rocket Money:

Besides tracking spending and managing budgets, this app also helps users track subscriptions to cancel those that are unwanted or unused. You can connect with service providers to negotiate lower rates, but the app charges a fee if they successfully lower a bill.

YNAB:

Short for “You Need a Budget,” this digital platform serves those who prefer zero-based budgeting. Users track every dollar to specific categories before they spend their income.

Besides these digital tools, many users of all ages transfer funds from one person to another with cash apps like Zelle, Venmo, PayPal, and Cash App.

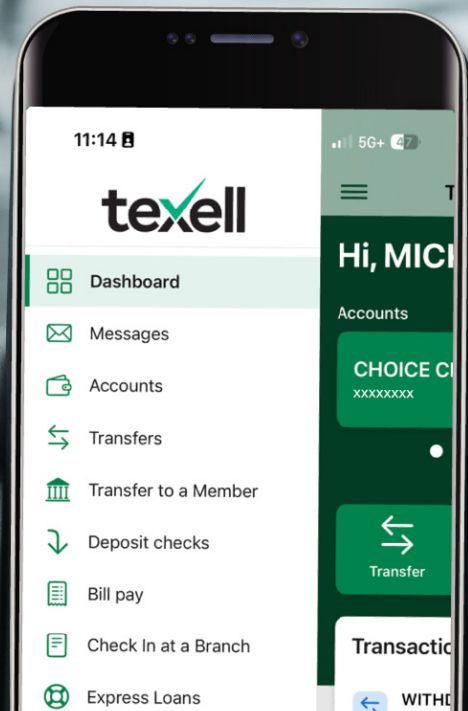
Choosing the right financial app

With so many options, navigating finances may seem overwhelming and confusing for younger generations, but there are digital tools available to meet their goals and financial needs. Keep in mind that the apps mentioned in this article may charge monthly fees for premium features. Take advantage of free trial periods to find those that work best for you. Texell members already have many of these convenient features within Digital Banking. To learn more about these tools, read Digital Banking Tools in this edition of Texell Quarterly.

Digital Banking Tools

By Kristen Reichert

For Texell members, Digital Banking lets you bank your way on your schedule. "We live in a digital age," said Sarah Wolfe, Texell's Digital Product Manager. "Gone are the days of long lines at the drive-thru on payday. With direct deposit, debit cards, automated bill payments, and many online features, you can bank from anywhere."



As technology advances, the app makes financial management quick, convenient, and secure. Encryption and biometric logins like face ID or fingerprints increase the security of accounts. You can set alerts for when a user logs in from a new device or changes information, and you can set up account alerts based on the account balance or transaction amount. If you need to dispute a transaction, you can submit the request quickly in Digital Banking.

Besides these security features, Digital Banking has tools located under Insights to set a budget and financial goals. The Credit Score & Report feature provides a snapshot of your credit score and includes tips to improve it. You can also apply for a loan, access Texell Insurance policies, and view and redeem BONUS Reward Points. Members can customize the dashboard for easy access to the tools they use most often.

"The goal for our Digital Banking team at Texell is to make sure every option is available for self-service for those who are not able to make it in person to visit our amazing staff at a branch," Sarah said. "We want to allow members the smoothest and simplest process to access their accounts."

For those who prefer to speak with one of Texell's Member Service Agents, contact information can be found at the bottom of the main dashboard to call, send a secure message, or find the nearest branch. To learn how to download the app, enroll, or for how-to videos, visit Texell.org/digital.

5 pro tips to keep accounts secure:

1. Set up the Digital Banking app to auto-update. This ensures that it functions properly and has the latest security features.
2. Set a secure password and log out when you're not using the app.
3. Don't share your password or account information with anyone you wouldn't trust with your money.
4. Don't shop online on unsecure sites or those you aren't sure you can trust.
5. Be aware of scams. Texell will never ask for your password or account information.

FROM THE FE

The Evolution of Digital Banking By Kristen Reichert



Since its establishment nearly 250 years ago, banking and the financial industry in the United States evolved to keep pace with technology. In 1781 Alexander Hamilton wrote to Robert Morris, the superintendent of finance for Congress, to advocate for a federal banking system: "Most commercial nations have found it necessary to institute banks and they have proved to be the happiest engines that were ever invented for advancing trade."¹ The Bank of North America in Philadelphia became the first chartered bank by Congress a few months later. After being appointed as the first U.S. Secretary

of the Treasury in 1789, Hamilton set up the first national bank. He defined the U.S. dollar in terms of gold and silver. The establishment of a national bank, the Bank of the United States, led to the rapid growth of the financial system and led to the rapid growth of the economy in the 1790s and into the turn of the 19th century.

From this beginning, banking has undergone significant changes. After the establishment of the Federal Reserve in 1913, Congress created the Fed as the central bank to manage the stable monetary system.

¹ [The US Banking System: Origin, Development, and Regulation](#) by Richard Sylla from The Gilder Lehrman Institute of American History

D TO FINTECH



up the federal revenue system, and silver coins, and founded ed States. Establishing this yth of the U.S. economy in the ntury.

ergone many changes, including rve System, or “the Fed,” in 1913. ral bank to provide a safer, more

FINTECH

In 1915, the Fed operated a funds transfer system, known as Fedwire, allowing banks to conduct wire transfers of funds the same day as requested. Today, the FedNow® Service is an instant payment infrastructure where members at participating financial institutions can send and receive instant payments in real time, 24/7.

How Computers Revolutionized Banking

By the mid-20th century, banks faced a new challenge: Growth. Between the 1940s to 1950s, the use of checks doubled, which overwhelmed bank clerks who handled each check about six times during processing. With accounts growing at 23,000 per month in 1950, banks had to close their doors by 2 p.m. to finish processing that day’s postings.

To solve this problem, Bank of America hired the Stanford Research Institute (SRI) to build the Electronic Recording Machine, Accounting (ERMA). While building ERMA, they invented Magnetic Ink Character Recognition (MICR) so that humans and machines could read account numbers.

By 1966, 12 regional ERMA centers served 97% of Bank of America’s 900 branches, marking one of the earliest examples of banking automation. What once required a vast number of clerks could now be completed significantly faster and with greater accuracy.

The Rise of Electronic Payments

The next major transformation came in the form of electronic payments. The invention of credit and debit cards in the 1950s, along with Automated Teller Machines (ATMs), brought the next innovation by providing instant access to funds anywhere, anytime. Barclays opened the first ATM in London on June 27, 1967. To learn more about this era of banking history, read [Taking a Closer Look at ATMs & eATMs](#) from our [July 2025 Quarterly](#). *(continued on the next page).*

Timeline of Banking Technology

1781

Bank of North America

1791

Bank of the United States

1913

Federal Reserve established

1915

Fedwire

1935

Banking Act established FDIC

1950

ERMA & MICR

In 1972, the Automated Clearing House (ACH) network was created by the Federal Reserve Bank of San Francisco to replace paper checks. With ACH, paper-based transactions shifted to an electronic check-clearing system, increasing the efficiency of payments. Today consumers worldwide commonly use direct deposit, online bill paying, and other ACH transactions.

Introducing At-Home Banking

In the 1980s, technology evolved to provide at-home banking tools which seems ordinary today, but was revolutionary at the time. United American Bank partnered with Radio Shack to offer the first home banking system using TRS-80 computers and secure modems. That same year, Bank One's Channel 2000 software allowed customers to view balances, pay bills, and transfer funds over phone lines with information displayed on a television screen. The first online banking system came from Chemical Bank, which released Pronto in 1983 and connected

computers to phone lines and TVs. Chase Manhattan Bank introduced a more advanced system called Spectrum in 1985, allowing users to make transactions, including buying and selling stocks, from their home computers.

The real breakthrough arrived in April 1993 with the launch of the first widely available web browser. Banks and credit unions began creating their websites with Stanford Federal Credit Union launching the first internet banking site in 1994. Other financial institutions followed suit with 32% offering online banking by 2000.²

Smartphones Provide Financial Management 24/7

With the internet boom in the 2000s and home computers becoming a necessity, more customers began using online banking. The rapid growth of financial technology, called FinTech, brought new digital services like online payments, budgeting tools, and investment portfolio management.

² [A Brief History of Digital Banking](#) from American Deposit Management

³ [Best Robo Advisors of 2026](#) from The Wall Street Journal.

FROM THE FED TO FINTECH



After Apple released the first iPhone in 2007, FinTech evolved to fill the need for digital banking apps. Ally Bank, founded in 2009, became one of the first major branchless banks where customers cannot access physical branches but conduct all their transactions online.

Besides banking apps, FinTech companies have developed other apps and desktop software to meet consumers' needs wherever they are. Learn more about financial apps and online services in Let's Talk Digital: Financial Tools for Gen Z and Gen Alpha in this issue of Texell Quarterly.

Artificial Intelligence (AI) Advancements

Today, the next phase of banking innovation is being driven by artificial intelligence (AI) and machine learning (ML).

Financial institutions increasingly use AI-powered models for credit decisioning, personalized recommendations, to automate routine decisions, and robo-advisers use algorithms to manage investment portfolios,

providing greater accessibility for a range of investor types. Betterment, Fidelity Go, and Vanguard are examples of apps with investment requirements as low as \$10 - \$100.³

AI is also playing a growing role in fraud prevention. As scammers use increasingly sophisticated tactics, financial institutions must also use AI tools for fraud detection to spot threats and block them immediately. ML models use pattern recognition and predictive analysis to spot unusual behavior, preventing fraud, phishing attempts, and identity theft. While AI tools are helpful, human oversight remains essential to ensure accuracy, transparency, and trust.

From "the Fed" to AI, banking has transformed and will continue to evolve as technology changes. Digital banking allows seamless, instantaneous transactions and the ability to monitor accounts, create budgets, set custom alerts, and more. To learn more about Texell's Digital Banking app, read DigitalBanking Tools.

Beware of AI Scams During Holiday Shopping

By Kristen Reichert

The days of asking family or friends for gift suggestions may be over as more shoppers are using artificial intelligence (AI) tools to find the perfect gift. According to eMarketer, over 37% plan to use AI for holiday shopping, including product and price comparison and for gift ideas.¹ However, criminals are also using the same AI technology to trick shoppers into buying non-existent gifts, sharing credit card information, and stealing personal data. As you prepare for the holiday season, be aware of these trending AI shopping scams.

Fake websites and products

Scammers build fake websites that feature AI-generated product images, fabricated customer reviews, and deepfake reviews claiming to be from celebrities or trustworthy sources. These sites also run convincing false ads for products that are never delivered. Others mimic auction sites with deeply discounted products and a countdown to when the deal expires, creating a false sense of urgency.

Buyer Beware Tip!!

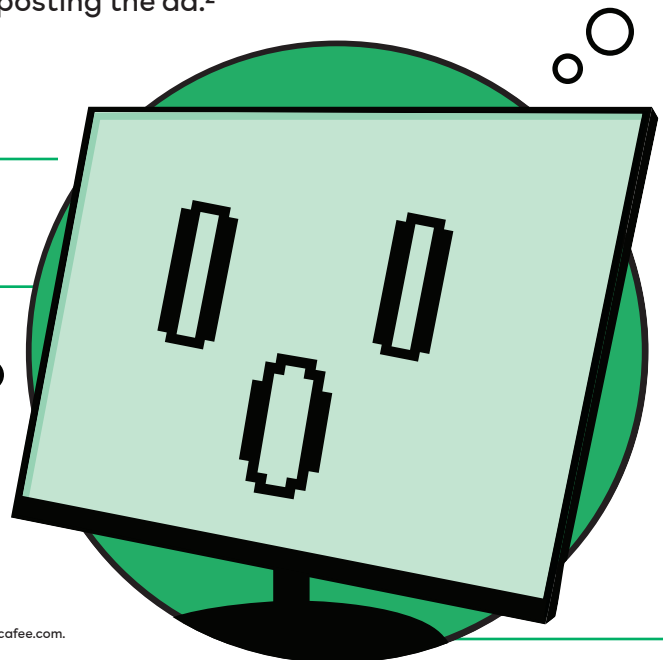
Before entering any payment information, review the domain name and search for reviews on customer feedback platforms like [Trustpilot](#) or the [Better Business Bureau](#).

Social media scams and deepfake ads

More consumers are shopping on mobile devices using social media platforms, but they have also become ground for scammers. Any criminal can post deepfake ads impersonating legitimate websites and products offering deep discounts. These “too-good-to-be-true” deals trick victims, leading them to a fraudulent website where criminals steal their credit card information as they attempt to make the purchase.

Buyer Beware Tip!!

When shopping on Facebook Marketplace and other reseller sites, be aware of AI being used to sell counterfeit goods. Facebook removes an estimated five to six billion fake accounts each year, so take a closer look at the profile or page posting the ad.²



¹ The 2026 holiday shopper is more deliberate and increasingly AI-guided by Arielle Feger from eMarketer.com.

² Actioned fake accounts on Facebook worldwide from 4th quarter 2017 to 4th quarter 2025 from statista.com.

³ Holiday Shopping Scams: What to Watch as Black Friday and Cyber Monday Approach by Brooke Seipel from mcafee.com.

Delivery and non-delivery scams

Package tracking has become part of everyday life, making delivery scams especially effective. McAfee found that 43% of people have encountered fake delivery notifications claiming the victim needs to enter credit card information to complete shipping.³ In “brushing” scams, victims receive packages they didn’t order that include QR codes to scan and register the product or for more prizes.

Buyer Beware Tip:

Verify delivery by contacting the carrier or using the official website’s contact information. Do not respond to text messages from unknown numbers and use a QR code reader to reveal the URL before opening the site.

Account verification scams

In these scams, the victim receives a text message or email claiming they need to verify account information. Scammers create a false sense of urgency to steal login credentials, payment information, or personally identifiable information (PII). The message includes a link to a fake login page or a phone number to call.

Buyer Beware Tip:

Don’t click links in messages or provide information over the phone. If you are suspicious about the request, search for the contact information on the legitimate website where you made the purchase to follow up.

Gift card payment scams

Gift cards remain one of scammers’ favorite payment methods because transactions are difficult to trace and to reverse. Scammers ask victims to pay for products using pre-paid gift cards, but they never deliver the product, and the victim loses the money paid. A scammer might also send a fraudulent message claiming they can’t process or deliver an item until the victim pays a fee using gift cards.

Buyer Beware Tip:

Legitimate websites and businesses offer several payment methods and wouldn’t limit options to gift cards only. Ignore requests from a third party to pay using gift cards and reach out to the business using contact information from their website.



AI customer service scams

AI tools aren't only used to bait shoppers into making a purchase, but scammers are now using these tools to dupe those who think they're interacting with customer service. Fake support chatbots, voice cloning in deepfake phone calls, and large language models (LLMs) writing personalized messages are all used to target victims.

Think twice before clicking "BUY NOW!" this holiday season

As you build your holiday shopping list this season, be aware of these scams that use AI to create deepfakes, fraudulent websites and ads, phishing messages, delivery scams, and fake chatbots. AI tools make these scams more convincing and harder to detect. Think twice before you click "purchase" – if it sounds too good to be true, it's most likely a scam.

If you think someone has compromised your account, contact your financial institution. Change passwords, enable multi-factor authentication, and monitor account activity.

Buyer Beware Tip:

If you didn't initiate the communication through the official website or help desk, ignore the message and do not share information. Legitimate businesses and companies will not ask for your password, PINs, or other personal information through an unsecured chat.

You can also report fraud to these government agencies:

- [Federal Trade Commission](https://www.ftc.gov/report-fraud)
at ReportFraud.ftc.gov
- [AI Complaint Form](https://www.atg.texas.gov/complaint-form)
at the Attorney General of Texas
- [FBI Internet Crime Complaint Center](https://www.fbi.gov/internet-crime-complaint-center)

Shoppers need to stay alert, diligent, and proactive to avoid scams. Read the Meet the Team article in this Quarterly for tips on how to protect your information and accounts from our Information Technology and Software Development teams.





Meet the Team

Information Technology & Software Development (IT & Soft Dev)

Learn what it's like to work at Texell in our Meet the Team series. This issue highlights two employees from the IT and Soft Dev departments, Marcel Yagyagan and Summer Owens.

Since October is Cybersecurity Month, this issue introduces two employees who make sure the credit union and members' information stay secure using the most technologically advanced systems. Growing up in Central Texas, Marcel Yagyagan didn't have formal IT training but was encouraged to apply by a current employee. Marcel has recently been promoted to IT Specialist II and has been at Texell for seven and a half years.

"My favorite project has been setting up the new headquarters," said Marcel. "It was fun seeing all the departments move over from the old headquarters and seeing how excited they were to get to set up a new desk."

Summer Owens moved to Texas from South Carolina and joined Texell in 2020 as a Teller at the Belton branch. She then helped start the Commercial department and became interested in Soft Dev while working on projects and seeing how systems behind

the scenes keep the credit union progressing. She moved to Soft Dev at the end of 2025 as the Software Development Project Manager.

"I took a project management course last year that made me realize I really wanted to focus more on that," said Summer. "Texell is really good about finding a job that fits you and people taking you under their wing and allowing you to learn."

"We've had a lot of managers or VPs who started as Tellers or Financial Service Specialists," Marcel agreed. "We have many departments from mortgage, lending, sales, insurance, marketing. We have it all. There's room for growth."

The IT and Soft Dev teams work together to improve the security of members' accounts and internally for the credit union. The software developers create applications and set up systems designed with strong security controls. *(continued on next page)*

Interested in joining a "Best Credit Union to Work For?"

Check out our current openings at: [Texell.org/careers](https://www.texell.org/careers).

These include access control, audit logging, data validation, and data encryption. IT teams maintain the servers, networks, and employees' devices that run the applications.

"Cybersecurity is a company-wide effort," Marcel said. "Every employee and every individual plays a role in protecting information, because even though our security has many layers of protection, like an onion, a single mistake, like clicking on a phishing link or reusing a password, could lead to a security event."

Marcel and Summer said they don't want anybody to be afraid of technology, but to build small, everyday habits to make them more resilient. Marcel compared it to putting on a seatbelt when you get into a car. They shared the following tips to avoid cybersecurity threats:

- ▶ Email accounts are the keys to your kingdom. If someone compromises your email, they can often reset passwords for many other accounts, so protecting it should be a top priority. Use a different email alias for every account you use so that if your alias gets compromised, you can shut it down without shutting down your primary email. Apple has a feature called "Hide My Email"
- ▶ Use a password manager and protect it like you would protect your bank accounts. Use a master password that has 20 or more characters made from random words with numbers, capitalization, and special characters. For all other accounts, use the password manager to generate a unique password of 20+ characters for each account.
- ▶ Enable multi-factor authentication, especially for email, banking, medical, and work accounts. MFA is an excellent second layer of defense even if an account is compromised. Biometrics and authenticator apps provide a stronger defense than email or text two-factor authentication.
- ▶ Don't overshare online or on social media by posting answers to security questions. Instead of using short answers, create phrases as answers to these questions.
- ▶ Be skeptical of unexpected emails, text messages, or phone calls asking you to click links or provide information. When in doubt, go directly to the company's website instead of using the link.

Cybersecurity isn't just online. There are ways to protect yourself when in public.

- Don't connect to public Wi-Fi. If you have to, ask an employee for the exact Wi-Fi name and never do banking, work-related activity, or any other sensitive work while connected. Using a VPN on your personal devices can help.
- Never use public USB ports to charge your devices, since these can be compromised by criminals.
- There are USB data blockers and charging-only cables, but using portable power banks is the best defense.
- Never leave your devices unattended, even if just for a minute to grab a coffee or use the restroom.
- Be wary of "shoulder surfers" trying to gather information from your screen.
- Turn off message previews on your lock screen. This hides personal information and MFA codes.



TAKE A BREATH

with Skip-a-Pay

By submitting a Skip-a-pay request, you authorize Texell Credit Union to advance your loan due date by one month on the loan(s) indicated and acknowledge that this may extend the maturity date of your loan(s). You also acknowledge that this request does not change your legal obligation to the credit union, that your loan agreement with the credit union provides for regular monthly payments, and that the credit union is merely informally permitting you to defer payment for the month(s) indicated. Interest will continue to accrue on the unpaid balance during the month you skip a payment. A \$25 processing fee for Skip-a-pays completed through Digital Banking or a \$35 processing fee for all other Skip-a-pays will be assessed for each loan you choose to skip a payment, and when payments resume, unpaid interest will be collected first. The processing fee is non-refundable and must be paid at the time your loan payment is skipped and cannot be rolled into the loan(s) balance. You acknowledge that Guaranteed Asset Protection (GAP) contracts allow for up to two (2) skipped payments or loan extensions per year over the life of the loan. Any additional skipped or extended payments will be deducted from the amount paid if a GAP claim is made. Express, Yes!, Employer, Home Equity, Home Improvement, Land, Mortgage, One-Time Payment, Fresh Start, Lines of Credit, Credit Cards and loans 15 or more days delinquent are not eligible for Skip-a-pay. Loans that have been 30 days past due within the last year are not eligible for Skip-a-pay. Loan payments must have been on time during the 3 months preceding this request and all accounts at the credit union must be in good standing. If approved, your regular monthly payment schedule will resume immediately following the month you indicate on your request form. No more than two, non-consecutive monthly payments may be skipped in a 12-month period.