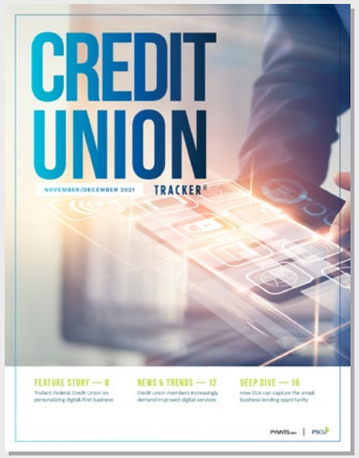
CREDIT UNION TRACKER®

DECEMBER 2021

PYMNTS.com | PSCU

Read the previous edition



■ NOVEMBER/DECEMBER 2021
Credit Union Tracker®

CREDIT UNION TRACKER®

PYMNTS.com | PSCU

ACKNOWLEDGMENT

Credit Union Tracker® was produced in collaboration with PSCU, and PYMNTS is grateful for the company's support and insight.

TABLE OF CONTENTS

EDITOR'S LETTER

Fraud concerns swept the nation as digitization accelerated during the pandemic. The uptick in online traffic and an increase in user profiles helped the virtual world become a breeding ground for bad actors. Fraud prevention service providers reacted accordingly, developing high-tech solutions to combat increasingly sophisticated fraudsters. Many organizations around the world quickly adopted these tools and offerings, while those that delayed innovating risked the financial and reputational consequences of security breaches.

These developments offered hard lessons for many credit unions (CUs). Their historical emphasis on personalized, face-to-face banking — however highly valued among members — left some unprepared to combat online fraud's worsening risks. Leaked credentials and insecure email networks — and those of vendors — serve as the main culprits for CUs' vulnerabilities on this front. PYMNTS' research shows that approximately 11% of credit union members turn to outside financial institutions (FIs) for products and services because they believe other institutions lessen their chances of having data stolen, and 9% of members do so because they believe other FIs have lower fraud risks. These perceptions could jeopardize both member retention and potential revenue as more consumers base their choice of financial providers on security.

CUs apparently are taking these lessons to heart: Recent PYMNTS' research shows that 93% of CUs are funding security, authentication or digital identity initiatives in 2021 — up from just 42% in 2020. CUs' investments in fraud management and anti-money laundering (AML) programs also are rising sharply. Our data shows that 69% of CUs are investing in fraud prevention innovations in 2021, a marked improvement from the 45% that did so in 2020.

As challenger banks and FinTechs continue to adapt to consumers' digital mindsets, CUs also must consider the many benefits of advanced tools such as data analytics, artificial intelligence (AI) and machine learning (ML). The implementation of these services can help to identify and eliminate the risks of fraud, reduce friction and improve member satisfaction in the process.

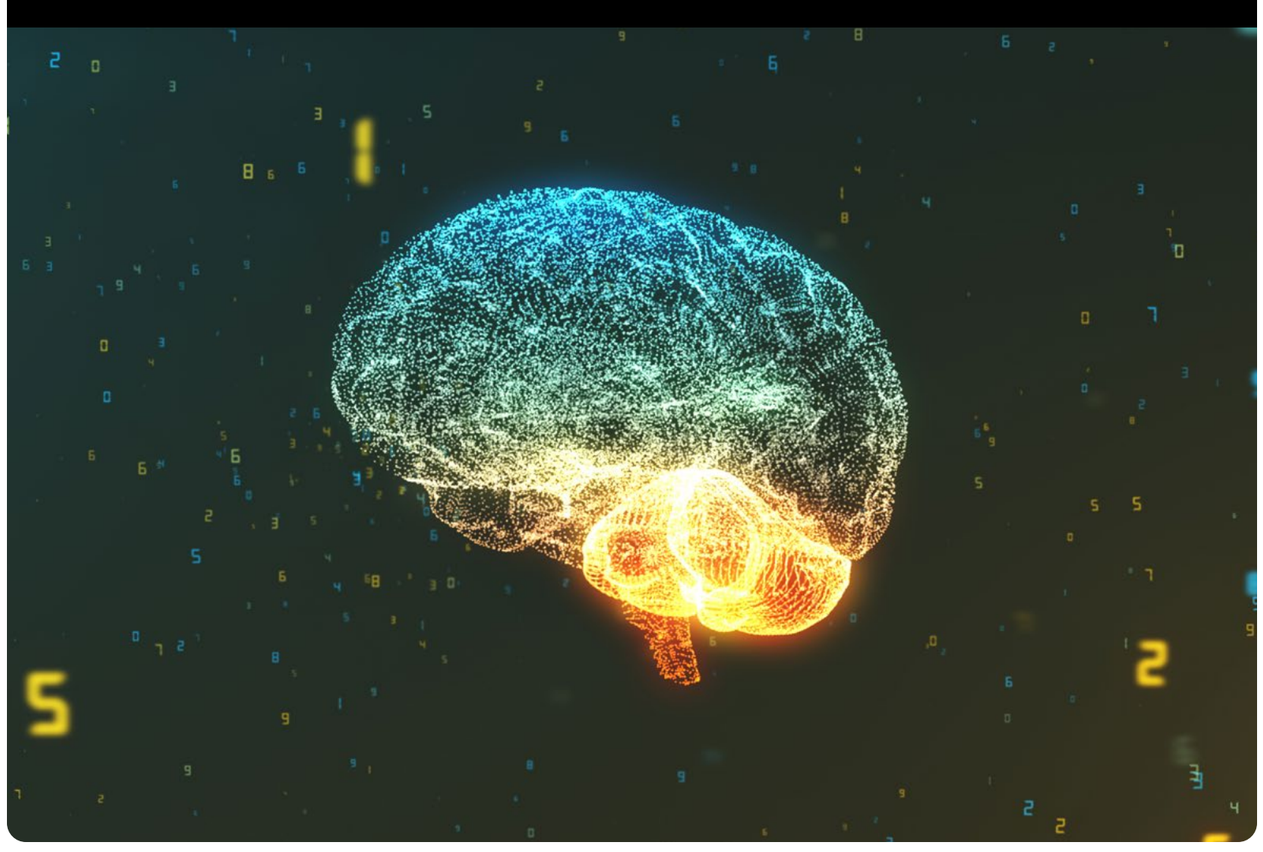
This edition of the Credit Union Tracker®, a PYMNTS and PSCU collaboration, delves into the current threats facing CUs and how innovative fraud prevention technologies can help them refocus on keeping members satisfied and loyal for years to come.

PYMNTS.com

Thought Leadership Team

Feature Story

How Advanced Tools Such As AI Can **Help CUs Curb Fraud In The Digital Banking Age**



FEATURE STORY

Technology has become foundational to society as the pandemic continues to impact all corners of the globe. Consumers have rushed to digital channels to tackle daily tasks including grocery shopping, handling healthcare appointments and meeting banking needs. As individuals focus on online platforms and mobile apps, organizations have been forced to follow suit or risk seeing consumers flock to digitally savvy competitors.

Few organizations have had to respond to this digital shift as rapidly as those in the banking sector, especially credit unions. Kelly Albiston, senior vice president and chief technology officer of digital product development at Mountain America Credit Union (MACU), explained that the volume of Paycheck Protection Program (PPP) loans and stimulus payments that passed through his company intensified its needs for infrastructural innovations.

"We have experienced a much greater need to enhance self-service experiences as face-to-face interactions became challenging during the pandemic," he said. "This includes continued investment in services like account opening and consumer lending applications, as well as [continuing to enhance] card-related services."

This trend is not exclusive to MACU, and some CUs opted to increase their investments in key services by merging. The National Credit Union Administration's (NCUA's) Insurance Report of Activity revealed that 43 mergers were approved in Q3 2021, nine more than were approved in Q3 2020. Twenty-eight of these mergers occurred because CUs wanted to expand their offerings, and eight could be attributed to poor financial conditions. CU merger rates are expected to continue rising in 2022 as smaller credit unions aim to expand the digital services available to their members by integrating with larger organizations.

DATA BREACHES POSE CHALLENGES

Digital expansions and mergers are boosting user accessibility and helping CUs meet members' new demands, but these shifts also have generated several challenges. Chief among them is fraud: More than $154 million in fraud losses were reported globally in 2020, and 56% of consumers in the United States claim they have been victims of fraud over the past two years.

"With all the data breaches in recent years leaking a lot of personal information into the wild, the know-your-customer (KYC) process continues to be challenging as [MACU] enhance[s] more self-service capabilities," he continued.

The rise in online profiles — combined with many consumers' less-than-ideal digital hygiene — has contributed to a steady increase in fraud. The issue has not gone unnoticed by credit union members, either. PYMNTS' data shows that 11% of CU members use tools and services from FIs other than their primary CUs because they believe their data is less likely to be stolen when they do. This means failing to adequately clamp down on fraud and neglecting to innovate could chip away at CUs' typically high member approval ratings.

"Keeping bad actors from opening accounts is challenging, but existing members are also at risk of falling for scams or having access to their accounts compromised by ever-evolving techniques used to gain passwords and intercept multifactor authentication PINs," Albiston said. "These threats, along with the speed at which money can now flow out from accounts through new channels, present a greater risk for fraud."

AI AND ML LEAD THE ANTI-FRAUD CHARGE

Fortunately for CUs, numerous ways to combat fraud exist and provide the personalized customer experiences members expect. Albiston said while some fraud is bound to occur, MACU's goal is to minimize the number of instances and their impact. Advanced technology now incorporates AI and ML to weed out fraudsters while creating minimal friction for genuine users. Part of this approach entails allowing the technology to better establish what constitutes legitimate member behavior based on members' histories and device usage.

"Like all security, it takes a very layered approach to be successful," he explained. "We use … identity services to establish our KYC processes, which have been very effective at minimizing account-opening fraud. We enhanced authentication services that profile member devices and prompt for step-up authentication from unknown devices."

Albiston also said implementing biometrics can help CUs distinguish bad actors from members and that tapping AI and ML to examine money movement across channels and even internally can enable credit unions to spot fraudulent traffic. Additionally, he said MACU supports credit-lock and account-creation tools that notify members in real time about access and changes to their accounts.

Credit unions are moving quickly to roll out digital innovations that can help them compete with FinTechs and digital-only banks, and some are partnering or even merging with other CUs to make these developments a reality. Keeping fraud to a minimum will be imperative as they make these shifts, however. There is no universal fraud protection formula for every institution, but leveraging AI, ML and other advanced technologies can give CUs more muscle to thwart sophisticated bad actors while keeping interactions smooth and convenient for members.

> "Keeping bad actors from opening accounts is challenging, but **existing members are also at risk of falling for scams** or having access to their accounts compromised by ever-evolving techniques."
>
> **KELLY ALBISTON**
> senior vice president and chief technology officer of digital product development at Mountain America Credit Union

Q&A

JACK LYNCH
Senior vice president and

PSCU

> WHILE **LEVERAGING TECHNOLOGY** IS CRITICAL, IT ALSO TAKES A HOLISTIC APPROACH THAT INVOLVES PEOPLE AND PROCESSES TO **EFFECTIVELY COMBAT FRAUD.**

Fraudulent activity and cyberattacks skyrocketed during the pandemic. How important is it for CUs to address fraud concerns now to prevent revenue loss and reputational damages in the future?

The battle against fraud in an evolving digital world is never-ending. The COVID-19 pandemic has been the 'great accelerator' for digital transactions, as consumer adoption of eCommerce [has] skyrocketed. These seismic shifts have greatly impacted fraud, and fraudsters continue to innovate and find new ways to attack using multiple channels and sophisticated fraud schemes. As credit union members continue to embrace technology and increase digital interactions, strong fraud management is more important than ever.

Establishing successful fraud mitigation strategies that strike the right balance between risk tolerance and member experience is imperative for credit unions. While leveraging technology is critical, it also takes a holistic approach that involves people and processes to effectively combat fraud.

Fraud will undoubtedly continue to evolve as consumers are increasingly gravitating to digital experiences, a trend that extends across all demographics. While different consumers may be utilizing digital in different ways, eCommerce and card-not-present transactions will continue to accelerate, [driving] online fraud numbers even higher. It is imperative for credit unions to have the right tools and technologies in place to stop fraudsters … while simultaneously ensuring a better member experience."

© 2021 PYMNTS.com All Rights Reserved

PYMNTS Intelligence

How Credit Unions Can Work To **Identify And Eliminate Fraud Risks**

Credit unions have been known historically for their member-first mentality and intimate face-to-face banking model. This business structure has worked in their favor, but it also has left some CUs less prepared for the pandemic-driven shift to digital-first banking and its associated risks — particularly the risk of online fraud.

Recent data revealed credit unions' specific vulnerabilities in this area, which include leaked employee credentials, insecure email networks and subpar software patch management. These weaknesses translate to an estimated yearly financial risk of direct fraud attacks that can range from $190,000 for small CUs to $1.2 million for large CUs. Indirect risks to CUs via their third-party vendors may be even more damaging. Technology solutions to these issues exist in the market, making it incumbent on credit unions to implement cybersecurity innovations to avoid potentially devastating effects on both revenues and members' trust. This month, PYMNTS examines the intensifying fraud risks confronting credit unions and the innovative technologies helping CUs mitigate these risks.

FRAUD RISKS AFFECTING CUs AND VENDORS

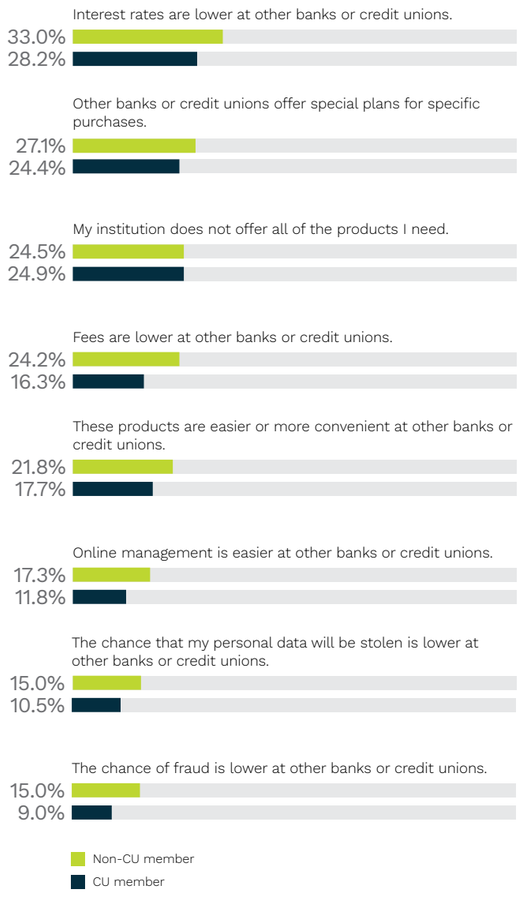
Vendors that serve credit unions are a key variable affecting fraud's overall impact on CUs. The financial risk of a third-party attack on a single vendor runs upward of $300,000 for small CUs and more than $1 million for large CUs, and that risk multiplies with each vendor that has access to a CU's sensitive data. Fraudsters frequently use leaked credentials to execute schemes such as ransomware deployment, and credit unions are relatively easy targets: Recent research indicated that 86% of CUs and 76% of their vendors had employee credentials circulating on the dark web. Out-of-date systems are another contributing factor to credit unions' fraud risk, as they left 48% of CUs and 58% of their vendors open to possible cyberattacks. CUs and vendors that do not innovate their operational systems make themselves more susceptible to hackers navigating well-known security gaps.

Consumer awareness also has led to increasing data security concerns. PYMNTS' research from August 2021 shows that 11% of CU members turn to other FIs for certain offerings because they feel those institutions reduce their chances of data theft, and 9% of members do so because they believe these other FIs offer a lower risk of fraud.

Member perception and brand reputation thus offer additional incentives for CU executives to implement strong cybersecurity measures. Greater numbers of consumers are deciding how to pay based on payment options' perceived security, according to a PSCU report. The share of consumers basing payment decisions on security doubled between 2019 and 2020 alone, from four in 10 to eight in 10. The same study showed

Figure 1:

Why consumers obtain financial products and services from secondary FIs
Share of consumers who cite select reasons for using financial products and services from secondary FIs, members versus nonmembers



that more CU members than nonmembers reported a charge dispute in the previous 60 to 90 days, at 25% versus 13%, respectively. CU members also were more likely to take advantage of mobile fraud alerts than their nonmember counterparts.

HOW CUs ARE LEVERAGING INNOVATIONS TO STRENGTHEN CYBERSECURITY

Legacy, rules-based fraud prevention systems are the most popular across the board for all banking institutions, with 40% of FIs using such equipment. Additionally, 26% still rely on antiquated manual reviews to identify fraudsters. Synthetic identity theft now is the fastest-growing financial crime in the U.S., and it poses an increasing threat to credit unions utilizing such weak fraud defenses.

AI and ML are among the technologies that CUs are leveraging to boost their risk management efforts. AI systems can sift through large quantities of data to guard against synthetic accounts without manual review, offering CUs valuable cost savings. CUs implementing AI platforms for fraud prevention can lower the occurrences of both false positives and human errors, reducing customer friction and freeing up staff to focus on improving the member experience.

CUs are working to catch up to other FIs' data security innovations to combat fraud. Recent PYMNTS' research shows that 93% of CUs are funding security, authentication or digital identity initiatives in 2021, up from just 42% in 2020 and a mere 35% in 2019. Investments to address fraud and prevent money laundering also have taken a sharp upward trajectory this year, following a drop in 2020. Though just 69% of CUs said they were investing in fraud prevention innovations in 2021, down from a recent high of 72% in 2018, this year's figure still represents a big improvement from 2020, when just 45% made these investments.

AI can help credit unions prevent fraud so that they can continue to do what they do best: delight members by meeting their demands and expectations. As fraudsters continue to innovate their avenues of attack, CUs may benefit the most from partnering with AI-based antifraud solution providers that can deliver strong security while optimizing the member experience.

Table 1:

Which new products and services CUs are funding
Share that cite select innovations as areas of investment, by year

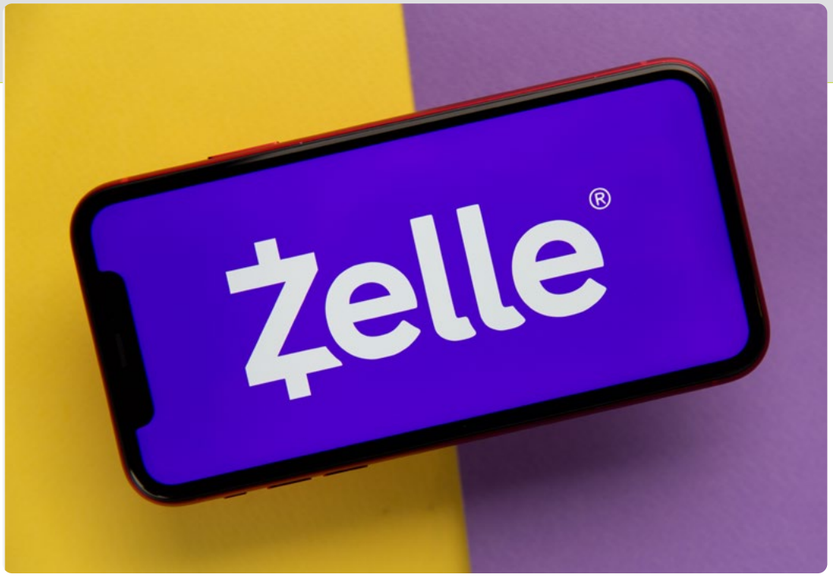
	2018	2019	2020	2021
Loyalty or rewards programs	29.4%	33.0%	77.2%	98.0%
Customized product offerings for members	21.6%	10.0%	44.6%	97.0%
Security, authentication or digital identity	48.0%	35.0%	41.6%	93.0%
Planning or budgeting tools	39.2%	9.0%	38.6%	85.0%
Mobile wallets	53.9%	54.0%	86.1%	80.0%
Fraud management and anti-money laundering	71.6%	69.0%	44.6%	69.0%
Mobile banking capabilities	0.0%	77.0%	70.3%	43.0%
Contactless cards	20.6%	31.0%	33.7%	42.0%
Small business credit	0.0%	24.0%	67.3%	36.0%
Voice assistants	0.0%	18.0%	11.9%	27.0%
Real-time payments	71.6%	76.0%	14.9%	10.0%
Installment credit	19.6%	50.0%	28.7%	7.0%
Small to mid-sized business payroll	0.0%	0.0%	4.0%	5.0%
P2P payments	40.2%	40.0%	26.7%	4.0%

CREDIT UNION **FRAUD**

REDSTONE FEDERAL CREDIT UNION SUFFERS BIN ATTACK

Fraud attempts are on the rise at larger FIs, including credit unions. Redstone Federal Credit Union recently reported a bank identification number (BIN) attack that impacted a small portion of its more than 650,000 members. These attacks occur when fraudsters obtain an institution's BIN — generally the first six digits of its issued debit card numbers — and use advanced software to try millions of combinations of the remaining digits to turn up legitimate card numbers.

In a press release following the incident, the CU said its fraud prevention team reacted immediately to mitigate and obstruct any further attacks. Many of the amounts processed on successfully breached accounts were less than $10, and CU officials said affected members would be reimbursed as quickly as possible. The incident followed a similar attack that affected Air Force Federal Credit Union earlier this year and highlights the growing fraud risks facing today's credit unions.



ZELLE FRAUD SCAM TARGETS CU MEMBERS

Popular peer-to-peer (P2P) payment service Zelle is a hot target for cybercriminals looking to cash out CU members' accounts, according to a recent report. Bad actors gain access through an elaborate phishing scheme that convinces genuine account holders to provide them with an identity-verifying code. The fraudster then uses this code to change the user's password and illegally transfer funds via Zelle.

Ken Otsuka, a senior risk consultant at CUNA Mutual Group, said he and his team learned that a number of CUs witnessed this particular scam in the same month they introduced Zelle into their payments operations. Fraudsters targeted CUs with other P2P offerings but appeared to prefer

Zelle because of the speed with which they received payments. Otsuka explained that attacks occurring over the course of a single day or several days can rapidly accumulate large fraud losses due to the sheer number of members in CUs' databases.

INNOVATIVE CU SERVICES AND SOLUTIONS

CUs ADOPT CLOUD SOLUTIONS AS DIGITAL-FIRST PRESSURES MOUNT

Credit unions are eyeing moves to the cloud in droves as both workflows and member expectations evolve. Some experts say steady cloud adoption based on a CU's specific needs may be preferable to an all-or-nothing approach, however.

CUs historically have shied away from the cloud because of existing legacy systems' complexity and their banking processes' specificity. Member satisfaction fell in 2020, however, sparking a wave of digital transformations as rival FIs threatened to outcompete CUs on innovation. Three-quarters of U.S. consumers now use mobile banking, and 20% of CU members plan to decrease their in-branch visits indefinitely. As a result, 42% of CUs now are committing to cloud solutions and an additional 54% are "curious" or "considering" migration.

The cloud offers three key benefits for CUs. The first is scalability, as it allows CUs to expand service offerings as needed to maintain member satisfaction without making a major investment in one shot. The second

benefit is cloud technology's ability to provide the continuous availability of data and services that CUs will need to best serve their members. The third benefit is affordability, as CUs can choose cloud services that best suit their business models without breaking the bank. To move operations to the cloud safely and securely, CUs should evaluate their workflows to determine what needs to remain on-site and how technology can help streamline the process.

PSCU ROLLS OUT IDENTITY INTELLIGENCE SOLUTION TO IMPROVE PERSONALIZATION, FRAUD DETECTION

Heightened competition is prompting FIs around the globe to reassess their uses of data and analytics to improve performance, growth and customer service. In response to the demand for such technology, credit union service organization PSCU is releasing Identity Resolution, a new "identity intelligence" solution as part of its revamped data science and analytics portfolio.

The solution is one of three data-enrichment strategies designed to improve FIs' targeted marketing response while also offering better credit bureau scoring validation and authentication to help prevent and detect fraud. The software seamlessly integrates with its users' content networks, simplifying adoption and improving member experience.

"PSCU and our team of data scientists understand how to harness the convergence of digital and data to provide greater insight into cardholder activity and preferences, and our refreshed data science and analytics portfolio helps analyze collective enriched data to create a holistic view of behavior to drive actionable insights," according to Jeremiah Lotz, managing vice president of digital and data at PSCU. "Through these resources, we are ultimately empowering our financial institutions to anticipate their needs and drive in-demand personalized experiences."

CREDIT UNION TRACKER®

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

ABOUT

PSCU

PSCU, the nation's premier payments CUSO, supports the success of 1,900 credit unions representing nearly 7 billion transactions annually. Committed to service excellence and focused on innovation, PSCU's payment processing, risk management, data and analytics, loyalty programs, digital banking, marketing, strategic consulting and mobile platforms help deliver possibilities and seamless member experiences. Comprehensive, 24/7/365 member support is provided by contact centers located throughout the United States. The origin of PSCU's model is collaboration and scale, and the company has leveraged its influence on behalf of credit unions and their members for more than 40 years. Today, PSCU provides an end-to-end, competitive advantage that enables credit unions to securely grow and meet evolving consumer demands. For more information, visit www.pscu.com.

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at feedback@pymnts.com.

DISCLAIMER

Credit Union Tracker® may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.