Sunwest Bank®

BUILT FOR ENTREPRENEURS BY ENTREPRENEURS

SUNWEST BANK NEWSLETTER | JULY 2023

Market Data

Interest Rates	Current	Month Ago	Year Ago
Bank Rates (As Of 6/30)			
WSJ Prime	8.25%	8.25%	4.75%
1 Month Term SOFR	5.11%	5.15%	1.60%
Fed Funds Rate	5.07%	5.08%	1.58%
30 Year Mortgage Fixed	6.71%	6.57%	5.70%
Treasury Rates (As Of 6/30)			
10 Year	3.81%	3.69%	2.98%
7 Year	3.96%	3.75%	3.04%
5 Year	4.11%	3.81%	3.02%
3 Year	4.48%	4.11%	2.99%
1 Year	5.40%	5.21%	2.77%
1 Month	5.19%	5.21%	1.30%
1-Month SOFR Term SOFR Swap Rates (As Of 6/30)			
10 Year	3.50%	3.37%	2.76%
7 Year	3.64%	3.42%	2.72%
5 Year	3.84%	3.54%	2.75%
3 Year	4.29%	3.87%	2.85%

Inflation Data	Current	Month Ago	Year Ago
CPI Headline YoY	4.1%	5.0%	8.5%
CPI Core YoY	5.3%	5.5%	6.0%
PPI Headline YoY	1.1%	2.3%	11.1%
PPI Core YoY	2.8%	3.3%	6.8%

Economic Data	Current	Month Ago	Year Ago
PMI Manufacturing	46.3	48.5	52.4
PMI Services	54.1	55.1	51.6
Case/Shiller U.S. Home Price Index	301.1	297.2	301.8
Housing Permits	1,496k	1,417k	1,708k
Housing Starts	1,631k	1,340k	1,543k
Retail Sales	$599b	$597b	$594b

LETTER FROM THE PRESIDENT

Building a Robust Defense: Proactive Measures to Secure Your Business

Cybersecurity remains one of the greatest hidden risks facing businesses across the country. Over the past few years, companies have seen an unprecedented increase in every aspect of financial fraud, particularly check fraud, wire fraud, and ACH fraud. Fraudulent attacks take diverse forms, but the most common vulnerability is individuals within your company. The sophistication varies, but these attacks are primarily initiated through phishing scams or spear-phishing attacks, targeting key personnel within your organization.

Recognizing unsophisticated attacks is relatively straightforward with appropriate training, as they typically involve poorly written emails or texts impersonating important figures. However, the more disconcerting frauds are those executed by sophisticated cyber criminals that slowly acquire information about your company and employees, and then wait for the opportune moment to strike, such as when a key team member is travelling. These attacks can be prevented, but only by having best-practice controls, training, checks and balances, and callback procedures in place.

While it may be inconvenient, implementing proper cybersecurity procedures and controls at your company is crucial to prevent cyberattacks and protect sensitive financial systems and information. Here are a few important cybersecurity best practices we recommend:

- **Use strong, unique passwords for online business activities, avoiding easily guessable information, and change passwords every 90 days.**
- **Enable Multifactor Authentication (MFA) for email, logins, wire releases, ACH release, and other monetary transfers and transactions.**
- **Regularly update software, including operating systems, web browsers, and business banking applications, by routinely installing patches and updates from software vendors.**
- **Install up-to-date antivirus and antimalware software on all computers.**
- **Conduct business banking only on secure networks. Avoid public Wi-Fi by using Virtual Private Networks (VPNs) or trusted wired connections instead.**
- **Implement dual approval for high-value wires and ACH transactions.**
- **Do not send and receive payment instructions to and from your vendors and customers in an unencrypted/unsecure manner. If you receive payment instructions via email, call them using an existing phone number to verify stringent callback questions.**
- **Provide recurring cybersecurity awareness and training programs for employees.**

Unemployment Rate	3.7%	3.4%	3.6%
Non-Farm Payrolls	+339k	+294k	+364k

Equity Markets	Current	Month Ago	Year Ago
Indices (As Of 6/30)			
DJIA	$34,408	4.07%	10.65%
S&P 500	$4,450	5.43%	16.34%
NASDAQ	$13,788	5.24%	23.90%

Sports Fact of the Month:

In 2015, the St. Louis Cardinals were fined $2 million by the MLB after the FBI uncovered that a team analyst hacked into the Houston Astros' player database and email system.

covering phishing emails, social engineering, malware, and safe browsing practices. Encourage the reporting of suspicious activities.

At Sunwest Bank, paramount importance is placed on cybersecurity to ensure the safety of our client's funds. The bank has made substantial investments in robust cybersecurity systems for monitoring banking applications, databases, firewalls, and networks. Comprehensive training programs are implemented for all employees designed to test our team members and keep them vigilant.

Unfortunately, we are only as strong as our clients' internal processes and cybersecurity infrastructure. If their systems are compromised, it can jeopardize the credentials and information we use for validation. By banking with a personalized and highly tailored business bank, you have the added protection that we know you and your activity, however, AI is changing even this safety net. To combat this, we partner with a handful of firms to offer recommendations to strengthen our clients' defenses. We also provide regular cybersecurity training with timely information related to current threats and best practices, to our clients via email and video on our website.

Please reach out to your relationship manager or our online banking team if you would like to review the enhanced security options available to you and your team.

Online Banking Support
All Markets
onlinesupport@sunwestbank.com
O. 800.330.9890

John Wise
Director of Depository Services
jwise@sunwestbank.com
O. 714.730.4461

Claudia Bustos
Sr. Treasury Management Officer
cbustos@sunwestbank.com
O. 714.881.3072