Fall 2015

TM Forum

Your trusted online source for Treasury Management news

SWIFT Bank connectivity now a more viable option for mid-sized businesses

In this issue

Many treasury managers may want to take a fresh look at SWIFT reporting and messaging services. As a uniform and potentially more efficient way to connect to all of their banks, the international bank-owned consortium has introduced service packages geared toward middle-market companies as well as large corporate companies.

"Treasurers are always looking for ways to make their operations more efficient," says Sheryl Wilhelmy, international product group manager within U.S. Bank's Global Treasury Management Group. "They want straight-through processes for all of their financial flows with their various banking relationships, and SWIFT is a logical solution.

"The fundamental appeal of the SWIFT channel to corporations," Wilhelmy says, "is that it is bank-agnostic."

In addition, for treasurers at middle-market companies, viewing payments and cash flow in real-time is essential, and SWIFT reporting can enable that.

Developments in corporate SWIFT access

SWIFT, a non-profit consortium owned by its member banks, has come a long way. For most of its 38-year history, SWIFT served only its member banks. But in 2001, SWIFT established the "Member Administered Closed User Group" (MA-CUG), which allowed select corporations (generally multinationals) to run a messaging system that banks could join.

In 2007 SWIFT introduced a new service called the Standardized Corporate Environment (SCORE). SCORE allowed large publicly held corporations to communicate directly to SWIFT member banks, and brought greater standardization of message types. Corporate eligibility for SCORE expanded two years later, allowing essentially any company, including privately held ones, to use the service.

continued on page 2

usbank

Still, the economics didn't make sense for middle-market companies. In response, SWIFT developed a lower-cost service called "Alliance Lite" that is more appropriate for companies with less message traffic. Even more recently, SWIFT introduced "Alliance Lite2", which offers cloud-based connectivity.

As with other SWIFT corporate services, Alliance Lite and Alliance Lite2 enable treasurers "to communicate with their banking partners using a secure channel rather than logging into various banking sites or establishing a direct transmission connection with each of their banking partners," Wilhelmy explains.

Meeting lower-volume needs

The fee structure makes Alliance Lite2 potentially viable for corporations with as few as two or three banking relationships. Geared to companies with as few as 200 messages a day and suitable for connecting customers who send and receive up to 10,000 messages per day, Alliance Lite2 supports both manual message entry and automated message flows.

Alliance Lite and Alliance Lite2 enable treasurers "to communicate with their banking partners using a secure channel..." Wilhelmy explains.

The basic requirements are a PC or laptop, the Internet Explorer browser, and a broadband Internet connection. The security system involves the use of a USB token supplied by SWIFT that is associated with the user's password. Users looking for an alternative to Internet-based connectivity can employ a SWIFT-administered virtual private network (VPN), although that approach requires additional hardware. Alliance Lite2 is designed to integrate with front- and back-end applications, payment and banking systems, as well as ERP systems.

"With SWIFT, you're removing the front-end graphical user interface application and channeling raw data," Wilhelmy says. "The treasury workstation or the ERP system creates the transactions and delivers them straight through to the bank."

With SWIFT bank connectivity, treasury workstations continue to give treasury managers the ability to conduct analyses, cash flow forecasts, research and transaction investigations, as well as execute non-standard payments, Wilhelmy notes.

Is SWIFT a good fit for your business?

Contact your Treasury Management Sales Consultant to learn more about SWIFT messaging and reporting services. U.S. Bank can help analyze your needs and consult with you on the best solution. ■■■

Utility customers appreciate convenience of having multiple bill payment options

Utility companies and other businesses with consumer customers often find that offering multiple payment channels can streamline payment acceptance and provide added convenience for consumers.

A relatively large number of U.S. households seek alternative ways to pay utility and other bills. A 2013 Federal Deposit Insurance Corporation survey found that nearly 8 percent or almost 10 million of U.S. households were unbanked (having no account at an insured banking institution) and 20 percent or almost 25 million were underbanked (having one bank account, but also using alternative financial services outside the banking system). Most underbanked households reported having an account only to receive direct deposit payments from employers.*

U.S. Bank E-Payment Service provides utilities and other businesses new ways for their customers to make payments using cash, checks and cards, either on-site at customer payment centers or at other locations.

"Since introducing our E-Payment Service 12 years ago, more than 100 utilities (private and government) and more than 300 other customers have used it to collect payments from their customers," says Stephen Stradal, vice president and commercial product manager within U.S. Bank's Global Treasury Management Group. More than 150 million individual customers have initiated payments in the E-Payment Service during that time.

continued on page 3

E-Payment Service includes Internet, touch-tone telephone (IVR), staffed service center and internet payment channels. Two newer E-Payment Service solutions, the Kiosk Channel and Walk-In Cash Payment Channel, add to those options.

E-Payment Service Kiosk

Many utility companies report challenges in collecting walk-in payments from customers. Walk-in customers may be unbanked or underbanked and want to make payments in cash on or near their billing date, thereby placing increased demand on staff and increasing wait times for other consumers. Conventional walk-in payments require staff time and are likely to involve handling large amounts of cash or checks that are at risk for error or theft. Often, customers making payments must wait in line for service, which is inconvenient and delays service to other customers.

The E-Payment Service Kiosk Channel reduces wait time and improves service by freeing up staff from accepting payments. Cash, check, debit and credit card payments can be accepted at the kiosk. Our research indicates that consumers prefer the convenience and speed of the kiosk with its easy-to-use interface and receipt generation capability. Companies may also choose to accept real-time payment confirmation messages for payments initiated at the kiosk, giving them just-in-time data to make informed customer servicing decisions. Kiosks can offer multilingual capabilities and be placed in locations that allow for 24-hour access.

From a biller's point of view, the E-Payment Service Kiosk reduces processing costs and delays, minimizes the risk of human error, and decreases shortages associated with cash handling. Billers can access insightful reports, track payments in real time and improve their cash flow. U.S. Bank offers on-site and remote maintenance of the kiosks, and also offers optional armored courier service. Billers simply need to replace printer paper and handle paper jams, should they arise.

The E-Payment Service Kiosk can be customized to reflect a biller's logo and brand, and is available in both indoor and outdoor models. "We now offer a smaller indoor tabletop model which is about half the size of the indoor kiosk, making it ideal for locations with limited physical space," Stradal notes.

E-Payment Service Walk-In Cash Payment

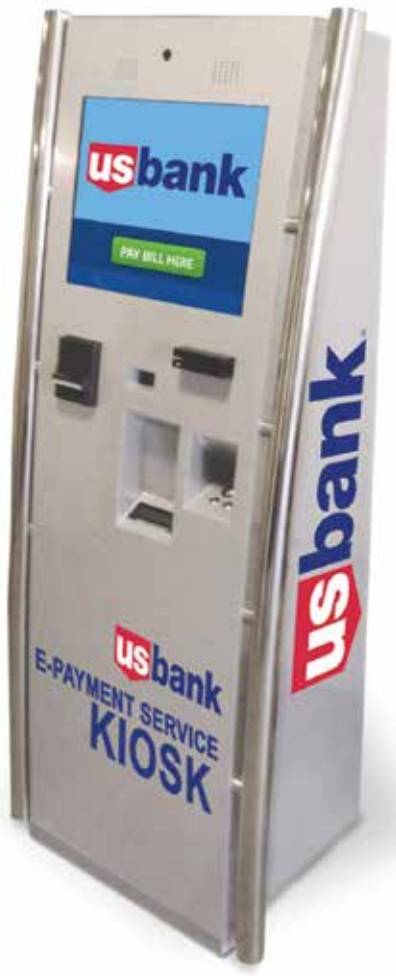
U.S. Bank is now piloting the E-Payment Service Walk-In Cash Payment Channel, which allows bill payment with cash at select convenience stores, drug stores, gas stations and other participating retail locations. This channel can complement a biller's kiosk payment acceptance capability beyond its own office locations by extending "payer present" capabilities and providing added convenience for payers.

By choosing E-Payment Service Walk-In Cash Payments, utilities and other companies can have the convenience of consolidating these payments, settlements and remittances with those initiated using other payment channels in the E-Payment Service suite. This can reduce the number of payment collection vendors needed, decrease the processing costs, and increase efficiency.

The E-Payment Service Walk-In Cash Payment channel is scheduled to be made available to clients in early 2016.

To learn more about U.S. Bank E-Payment Service collection alternatives, contact your Treasury Management Sales Consultant. ■■■

* 2013 FDIC National Survey of Unbanked and Underbanked Households, Federal Deposit Insurance Corporation, October 2014. https://www.fdic.gov/householdsurvey/



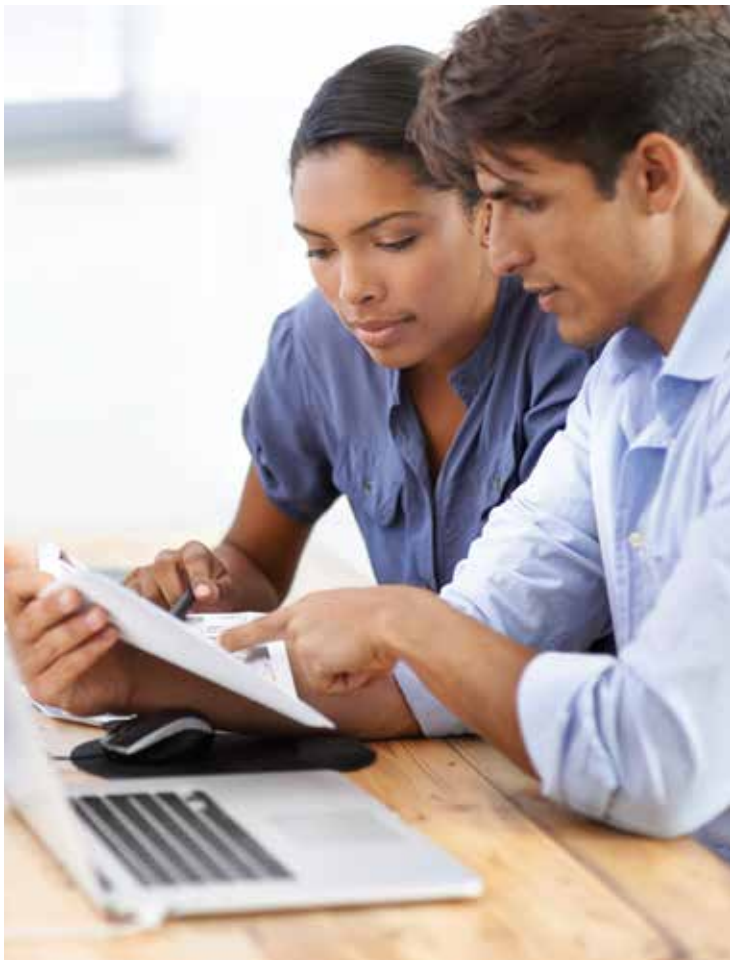
Keys to preventing payments fraud: vigilance, adopting best practices and risk mitigation services

Payments fraud continues at disturbing levels — with 62 percent of companies responding to the Association for Financial Professionals' 2015 Payments Fraud and Control Survey that they were targeted in the last year.

"This annual survey is notable in its consistent message that fraud remains a crime of opportunity, and plenty of opportunities continue to exist for both internal and external parties to commit fraud against businesses large and small," says Steve Helgen, vice president, risk management in Global Treasury Management at U.S. Bank.

Email spoofing scams

Helgen points to a heightened threat from social engineering and email spoofing. "This is a relatively low frequency but high impact fraud scheme, where a business's email system is either compromised or a criminal is able to make it appear as if the email is coming from a key officer of the company," he explains. "The email directs an employee to wire funds immediately to a specific account, often overseas."



With this type of scam, which is sometimes referred to as "masquerading" or "impostor fraud," there is also frequently a request of confidentiality on behalf of the key officer (CEO or CFO), which helps the criminal evade some controls.

Cyber fraud prevention strategies

The AFP study highlights a number of strategies that companies are using to thwart cyber fraud, including:

- Daily reconciliation of transaction activity
- Adopting a stronger form of authentication or added layers of security for access to bank services
- Implementing systems to ensure that disaster recovery plans include the ability to continue with strong controls and maintain in-office compliance when enacting in a disaster recovery
- Upgrading authentication procedures and devices used to access their networks
- Requiring use of company-issued laptops when initiating payments through company networks
- Dedicating a PC for payment origination (with no links to email, web browsing or social networks)

"Dual control, where one individual initiates the transaction or batch and another approves it, remains a key control strategy, and it is surprising that companies still balk at using it," Helgen adds. "It's also critical that the second person actually verifies the transaction rather than assuming that if the other individual created the transaction it must be okay."

Malware continues to be a problem, he says, but criminals have discovered that many banks and their customers have bolstered their ability to detect malware, so they are switching their approach. Nevertheless, Helgen strongly recommends that business customers take advantage of the IBM® Security Trusteer Rapport™ anti-malware software that the bank makes available to them, at no cost, via SinglePoint®, the bank's Internet treasury portal. "This software is easy to download directly from SinglePoint and should be installed by all SinglePoint users," he suggests. "It can disable malware on a user's computer — offering much stronger fraud prevention than anti-virus software."

continued on page 5

Check fraud still the top threat

The AFP survey confirmed once again that checks remain by far the most targeted payment method.

The "gold standard defense" against check fraud continues to be Positive Pay with Payee Verification. U.S. Bank's most recent enhancement to this service is a virtually "continuous/immediate" update capability for issue maintenance on SinglePoint. "Customers can upload newly issued checks through SinglePoint and be assured that the payee will be able to cash the check at a U.S. Bank branch without being concerned about being turned away," Helgen says.

Another service that is very effective is the check block or filter. Most customers use this as an actual check block, but it can be used as a filter as well, so that a check over a pre-set amount is automatically returned. "This is a terrific fraud prevention tool that can be used on deposit-only or rebate accounts, where the dollar size of the checks is predetermined, as well as on accounts where no check disbursements are planned," he advises.

U.S. Bank strongly endorses the use of daily reconciliation as a fraud detection measure, although this practice typically only detects fraud after it has occurred rather than before it happens — as can be accomplished by Positive Pay and check filters. "Nevertheless, daily reconciliation can be an effective tool to use on accounts where very low volumes of checks are written each day," Helgen says. "The downside is that this process does not provide protection at the teller line."

Constant vigilance is needed

"These are all important tools and strategies," Helgen says, "but the biggest challenge is complacency — the idea that what we're doing is enough. It's important to remember that the perpetrators of fraud are adapting their tactics on a regular basis, and vigilance is desperately needed." ■■■