Fall 2017

TM Forum

Your trusted online source for Treasury Management news

In this issue:

2017 WORLD'S MOST ETHICAL COMPANIES® ™
WWW.ETHISPHERE.COM

Best Treasury and Cash Management Provider in the Midwest for 2017 — Global Finance

Five best practices for Same Day ACH expedited payments

Key considerations for your payment systems

We're rapidly approaching the reality of faster payments. After the Federal Reserve launched its Faster Payments task force in 2015, several options have been developed to make the payments process simpler, faster and more transparent, efficient, flexible and secure. The first faster payment option on the scene is also one of the fastest: Same Day ACH, which is an evolution of next-day traditional ACH.

Same Day ACH led the way with faster payments when credit origination began in September 2016. NACHA estimates that Same Day ACH credit origination totaled more than $17 billion in payments within the first three months of use.

With same-day debit origination scheduled for September 2017, it's important for organizations to review the implications for their business, identity opportunities to speed up payments and update their processes accordingly. Your security measures need to keep pace with the speed of your payments.

Follow these best practices to strengthen your organization's Same Day ACH processing:

1. Review ACH origination policies and procedures for both credits and debits

- As Same Day ACH is an opt-in service, you'll need to sign up to originate same-day payments. Signing up for same-day processing arms your payments staff with tools to address contingency situations (like missed payroll), process urgent refunds and settle same-day trading partner payments. There is no cost to opt in, and fees only apply if you use the service.
  - Remember: If you have already opted in for Same Day ACH credits, you will automatically be ready to originate debits starting on Sept. 15, 2017.
- Evaluate and update your customer and trading partner agreements and disclosures. Consider communicating any payment timing changes with your customers in advance, especially if you'll collect funds sooner than before.

Continued on page 3

Continued from page 2...

- Review and update accounts payable (A/P), accounts receivable (A/R) and payroll procedures to optimize the use of Same Day ACH. Address how to apply incoming Same Day ACH payments received late in the business day.

2. Review technical capabilities for Same Day ACH origination

- Review and update payment portals, online customer disclosures and authorization forms to ensure you are ready to initiate Same Day ACH payments when needed.
- Make sure your payment files meet the criteria for Same Day ACH; you will need to:
  - Monitor for the $25,000 per transaction limit.
  - Adjust current file effective dates and payment file delivery schedules.
- Make sure you can change effective dates in your files to prevent sending transactions earlier than intended. This is particularly important with Same Day ACH debits, where the receiver needs to have sufficient funds in their account.
- If you send your files via ACH Direct File Transmission, consider automated control totals for file confirmation where no control total manual entry is required. Automating this security step saves time to help ensure payments are processed by the earlier processing deadline required for Same Day ACH.
  - If you need to enter manual control totals, be sure to submit them well in advance of the noon CT deadline so payments are not delayed.

3. Review changes to your cash positioning

- Same Day ACH payments and settlement transactions post to your depository accounts at various times throughout the day, instead of the more predictable settlement times of normal ACH. Make sure to plan accordingly.
  - Same Day ACH credits may already be posting to your accounts and appearing in current day reporting later in the day than traditional ACH payments. When debit origination is implemented Sept. 15, 2017, you may need to have funds available in the afternoon if your trading partners debit you on a same-day basis.
- Make sure you are set up for current day balance reporting, which is updated at 7 a.m., 10 a.m., 2 p.m. and 5 p.m. CT. This will help you with cash positioning and reconciliation of Same Day ACH transactions posting to your account in the afternoon.

4. Review and strengthen fraud prevention measures

- Train staff to be vigilant and understand how fraudsters socially engineer and use business email compromise scams. With these scams, requests can appear to come from legitimate parties.
- Confirm that requests to add or change beneficiary payment account information are received from an authorized party. Verify requests to change beneficiary accounts through alternative communication methods, such as direct phone calls to known customer and trading partner contacts (for example, they email you the request, you call them to verify using an already established phone number).
- Use secondary approvals for trading partner account changes and carefully review urgent or unusual requests.
- Employ existing ACH fraud prevention tools — such as ACH Positive Pay, blocks and filters —with automated services like the free anti-malware software IBM® Security Trusteer Rapport®, which is available within our online banking portal. Users can access the portal via desktop, mobile and tablet devices.

Continued on page 4

Continued from page 3...

- Conduct a full review of banking portal administration rights to ensure that dual controls and authorizations are available on all payments and functions.

5. Recognize Same Day ACH as the first step in the faster payments evolution

- Same Day ACH represents just one of many changes to the payments landscape. Keep up to date on evolving faster payment options to craft a more efficient and cost-effective payment strategy.

Still have questions? Contact your U.S. Bank Treasury Management Consultant today.

What you need to know when deploying faster payments

Adam Kruis and Laura Listwan

While the future of payments is looking faster, rushing to get there only raises confusion and risk.

We hear many questions from our clients about faster payments solutions, often stemming from a need to understand the implications of making the move and not understanding the benefits beyond faster processing. Each major faster payments solution requires thoughtful analysis in a larger payments strategy — and some have unique systemic challenges to overcome.

If you're pursuing one (or more) of these solutions, here's what you need to know to ensure a smooth deployment.

Cross-solution implications

You may need to shore up your technical, transactional and informational processes depending on the solution you choose. Whether you deploy Same Day ACH, Zelle®, Real-Time Payments (RTP) or MasterCard Send/Visa Direct, keep these elements of your payments system in mind:

- Changes or upgrades to IT infrastructure. Can your current systems handle the increase in same-day (and instantaneous) transaction processing? How many systems in your infrastructure require upgrades to support the increase in payment velocity? Also, several of the new faster payment solutions require adherence to new standards; make sure you factor this development into your deployment costs.
- An understanding of transactional sizes and frequencies. Regardless of the solution, review the scope and payment amounts of your current transactions — especially if implementing a solution that limits processing to certain dollar amounts or time frames.

Continued on page 6

Continued from page 5...

- Changes in messaging. Will you have time and resources to train your teams on effective customer and trading partner messaging about the mechanics and benefits of any new solution? Mixed messages with internal and external sources can cause confusion, which could limit adoption and increase risk.
- Changes in treasury cash positioning. As new payment types are deployed, you'll need to look at how they might affect settlement times, funding times, and other crucial timing factors.

Should you pursue deployment, each major faster payments solution has its own unique implications. Let's look at specific elements for each of them.

Implications for Same Day ACH

Here's the good news with Same Day ACH: You won't need significant new development efforts to deploy it. However, you should still consider these items before expanding efforts.

- Timing of payment files. Same Day ACH windows are early in the morning and the afternoon. If you miss them your payments could move to the next business day. Can you ensure your same-day payments fall within those windows?
- Credits versus debits. Same Day ACH credits are already in place, with debits coming later this year. Customers don't always consider whether they are eligible to receive same-day debits, so frequent communication helps reduce any confusion.
- Size and frequency of current payments. Same Day ACH transactions are limited to domestic payments under $25,000. From a process standpoint, you should review your current payment types (especially wires and overnight checks) to see which traditional domestic payments could benefit from Same Day ACH settlement.
- Reporting structure. Same Day ACH best practices include setting up current day balance and automated totals reports, both to ensure confirmed settlement and to catch unforeseen transactions. Do you have ACH Positive Pay on your accounts to identify unanticipated debit transactions? Can your payment systems handle an increased reporting frequency?

Implications for Zelle

Zelle operates in its own network, though most major banks (including U.S. Bank) participate. Keep these items in mind when choosing to pursue Zelle payments.

- Availability of payee email accounts or phone numbers. Zelle uses an alias-based system, relying on payees' email addresses or phone numbers to process transactions. If this information is not already available in your systems, you will need to start collecting it.
- Authenticity of payee email addresses or mobile numbers. Even if you do have email address or mobile phone information, can you confirm that it's up to date? If not, you'll need to ensure that the information is validated periodically (especially prior to payment). Additionally, you will want to review who'll have access to make changes to these fields.
- Size and frequency of current payments. While the network does not have an established transactional limit, each receiving bank can establish its own limit for real-time payments. As these are irrevocable payments, you'll want to ensure accuracy of the payment instructions before sending them to your bank.

Continued on page 7

Continued from page 6...

- Payee types. Zelle supports consumer-based person-to-person (P2P) as well as business-to-consumer (B2C) payments, but does not support business-to-business (B2B) payments.
- Consumer awareness. You'll need to educate your staff on how to answer any payee questions — like when they can expect payment or when they might be solicited for enrollment information from either your organization or Zelle. Not all consumers will feel comfortable with this network, so you'll need to plan for alternative payment solutions.

Implications for MasterCard Send and Visa Direct

These networks carry a distinct set of implications from the other major solutions. Review these items before embarking on any debit card-based journey.

- Adherence to bank-created limits. While the networks have established transactional limits, each receiving bank can create its own transactional limit when processing MasterCard Send or Visa Direct payments. Since these limits vary and are subject to change across banks, you may want to limit the transaction value of the payments that your company sends through these networks.
- Compliance with Payment Card Industry (PCI) standards. Since you're dealing with card-based transactions, you'll need to factor PCI compliance into your workflow. Does your system have the ability to support the additional regulatory requirements?
- Consumer adoption. Some consumers won't feel comfortable with sharing their debit card numbers for transactional purposes, with good reason. Fraud concerns might prevent payment from card-based networks, so you'll need to plan for other options.

Implications for Real-Time Payments

As a new network, RTP carries new implications that don't apply to older networks. Here are elements to consider leading up to deployment.

- Company adherence to the ISO 20022 standard. Aligning with the international ISO 20022 standard requires translating your information to this format. This may require extensive changes to your existing IT infrastructure — unless your enterprise resource planning system already supports this format.
- Trading partner adoption of RTP. You aren't just working with your bank. You also need to consider if your vendors and/or business customers will be migrating to RTP. If so, they will also need to align with ISO 20022 for you to realize the benefits. Since this is a new network and adoption will be ongoing, you'll need to plan for alternative payment options.
- Review of receivables processes. RTP affects both sides of the payment process. Will your receivables system be able to process RTP with the same efficiency as the payables side? Will you need to update procedures/processes to support payments received on weekends and bank holidays?

At U.S. Bank, we're telling our clients that these new payment options should not replace their traditional methods, but rather supplement what's already in place. It's also just as important to identify which solutions wouldn't be a good fit, which can help avoid unnecessary cost and risk.

Continued on page 8

Continued from page 7...

Look before you leap

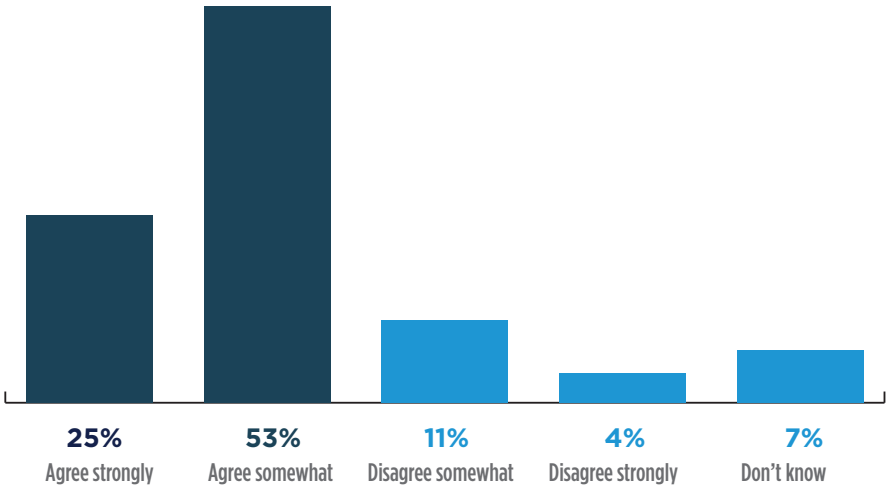
As we noted in our last post, no single solution offers a perfect fit for an organization's payment strategy. Review your current processes and determine how to use faster payments to your advantage without disrupting your current customer and trading partner relationships or internal processes.

Training employees to fight hackers

By now, finance executives know that cyber-thieves are constantly looking for ways to climb over, or burrow under, their firewalls. What they may not realize, however, is that the gate is frequently left unlatched – by their employees.

They're doing so inadvertently. It's not as if most employees are secret cyber-hackers, waiting for the day (their last one, retroactively) when they can set loose an email worm capable of compromising the company's proprietary data. In a recent survey about data security, in fact, the majority of finance executives, 56%, confirm that they view current or former employees as little or no threat. By comparison, 67% of respondents consider hackers or cyber-criminals to be a moderate or severe threat.

FIGURE 1 SECURITY GUARD
Our company has deployed the right technology to manage cybersecurity effectively.



Continued on page 10

Continued from page 9...

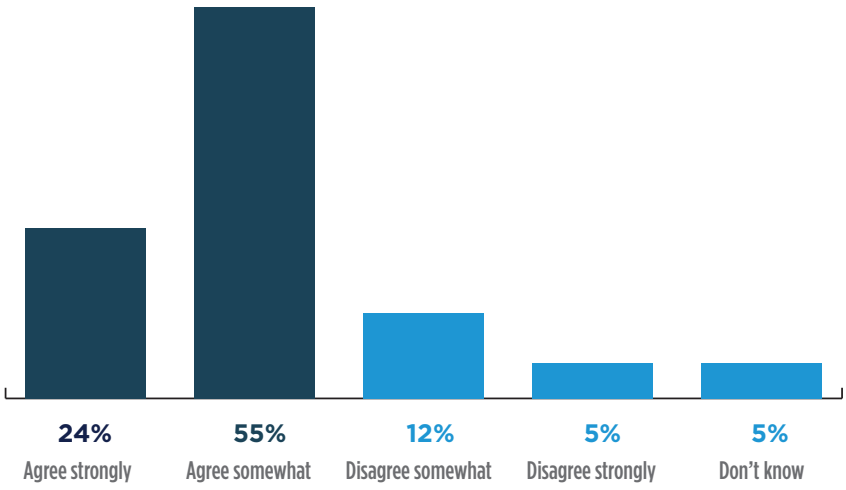
The survey, titled Cyber and Data Security in the Middle Market, was conducted by CFO Research, in collaboration with Visa and U.S. Bank. The online questionnaire drew 316 responses from U.S. finance executives, a plurality of whom hold the title of CFO, with controllers also amply represented. All respondents work at companies with annual revenue of more than $25 million and up to $500 million. The survey-takers represent a broad range of industries.

Survey-takers assessed several different aspects of their companies' awareness – and preparedness in terms of successfully guarding against cyber-intruders. In their answers to questions, finance executives offered evaluations of their companies' technological tools and skills when it comes to repelling hackers as well as how much of a priority it is for the management team and for employees.

Most respondents say they believe that their company's technology is up to the task of deterring hackers. More than three-quarters of respondents agree that their company has deployed the appropriate technology for effectively managing cybersecurity (see Figure 1). As one respondent urges "Maintain an up-to-date security system and monitor the same on regular basis in real time."

FIGURE 2 KNOW HOW

Our company has the technical expertise required to manage cybersecurity effectively.



A nearly identical proportion agrees that their company possesses the expertise to effectively manage the cyber-threat (see Figure 2).

Furthermore, the clear majority of respondents, 82%, agree that their company's top executives treat cybersecurity with the appropriate gravity and seriousness. Asked to identify the most important step a CFO can take to make the finance function less vulnerable to cyber-threats, one respondent writes: "Due diligence from the top and upper management." What matters most, offers another finance executive, is the "tone at the top… take security practices seriously."

Continued on page 11

Continued from page 10...

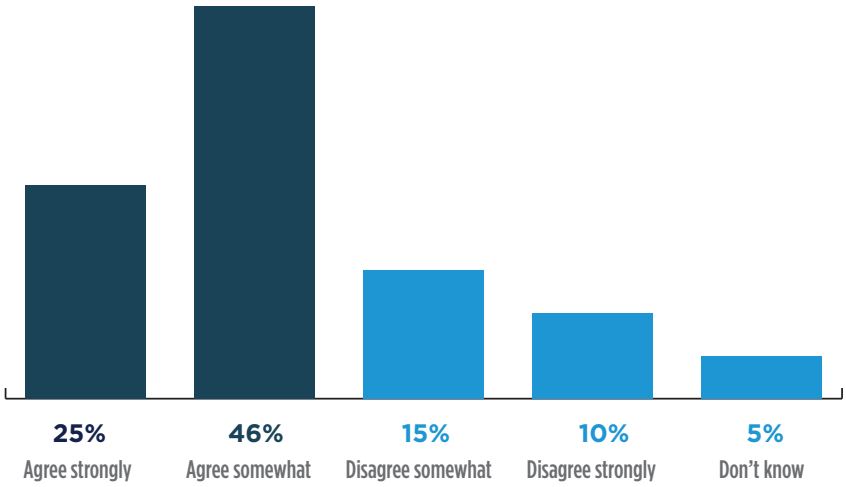
That admonition doesn't just apply to senior management. One survey-taker stresses the "need to be aware" and to "convey the importance (of cyber-security) to management as well as employees." Guarding against hackers needs to become an organizational priority, with every company member accepting accountability for deterring, detecting, and reacting to cyber-risks as they come up.

In the survey, just under one-quarter (24%) of respondents say they agree strongly that their "rank-and-file employees treat cybersecurity with the gravity and seriousness that it warrants." By comparison, 45% of finance executives agree strongly that their top executives approach the issue with the attention required.

In their written comments, as well as during follow-up interviews, finance executives drew a connection between employee awareness and outsider access. A critical tool for keeping the cyber-pirates from sneaking aboard is, as one respondent writes, to "make employees aware of the potential threats so that they can recognize and prevent them." One respondent's advice summarizes the issue simply: "Ensure that all systems are password protected and that staff is appropriately trained to look for these issues."

FIGURE 3 WORKING KNOWLEDGE

Our company/employees have access to training/education on recognizing cyber-threats and acting on them.



What can go wrong? As they become ever-more skilled at taking advantage of cracks in corporate systems, hackers can now target employees with emails that are close to dead ringers for those sent by colleagues or business partners–the phenomenon known as "phishing." At Temkin International, a manufacturer of plastic packaging products, an email from a vendor included instructions for wiring payment to them. "We wired the money," says Controller Dalan Andersen, "and we're still trying to figure out what happened. That's a fishy one." In any case, it's become clear that the vendor had nothing to do with it.

Andersen himself has received emails that "look exactly like they are coming straight from our owner. He keeps asking me to send him money by wire."

Continued on page 12

Despite the persistence of these emails, Andersen knows better. “I know he’s not the type to ask me to do that over email,” he says. He also knows that neither he, nor the company’s 400 employees, can depend on his instincts to fend off cyber-hackers. “The hackers are coming up with new stuff all the time, and I should know about it before it shows up in my inbox,” he says. “I read as much as I can. But I probably need to get better training.”

He’s hardly alone. Asked whether their employees have access to training/education about recognizing and acting on cyber-threats, only one-quarter of respondents say they agree “strongly” with almost half choosing to agree “somewhat.” Finance executives clearly see room for improvement (see Figure 3).

In their responses to open-text questions, respondents often suggest that employees must be made more aware of the policies and procedures they need to follow, from how they choose passwords (seven characters, combining alpha and numeric characters) to when they change them (every 60 days). One respondent’s checklist: “Change passwords regularly, make sure you don’t open spam or spoof emails and help support investments in cybersecurity.”

In the absence of seeing an easy way in, cyber-hackers will often choose to stay away.