New England’s source for industry advocacy, networking opportunities, education, news and information.

Securing Faster Payments
Mitigating Risk at the Speed of Fraud
Table of Contents

Executive Summary ................................................................. 1
The Faster Payments Landscape .................................................. 2
   Key Industry Players ............................................................. 3
      NACHA ............................................................................. 3
      The Clearing House .......................................................... 4
      The Federal Reserve ......................................................... 5
      Other Players Shaping the Industry ...................................... 6
Faster Payments Risk and Vulnerabilities ....................................... 7
   Operational Risk ................................................................. 8
   Cyber Risk ........................................................................... 8
Securing Faster Payments .......................................................... 10
   FedACH Services ............................................................... 10
   Onboarding and Monitoring .................................................. 12
   A Word about Third-Party Processors .................................... 13
   Behavior Analytics ............................................................. 13
   Transactional Analytics ....................................................... 14
   Software as a Service .......................................................... 14
   Service Suites ..................................................................... 14
Next Steps for Financial Institutions ............................................ 15
Summary .................................................................................... 16
Solution Providers ...................................................................... 16
Executive Summary

Faster payments are seeing explosive growth, and new methods for moving payments faster are emerging daily. With the rush to bring new faster payments to market, we must not overlook the importance of maintaining payments that are safe and secure—no matter how fast they move.

Sophisticated threats challenge and even bypass existing security controls, putting financial institutions and their customers or members at risk for significant loss and reputational damage. Some of today’s controls, such as back-end investigations and after-the-fact reports, are slow, costly and unlikely to recover funds in a faster payments world.

Keeping our payments system safe and secure is a top priority. The Federal Reserve’s Faster Payments Task Force said it well:

Before new, faster payments solutions are broadly adopted, the industry should embrace a security-first mentality. While it will never be possible to completely thwart ever-evolving payment security threats, implementation of these new, faster payment solutions present a once-in-a-generation opportunity for all participants (solution operators, service providers, financial institutions, government agencies, businesses and consumers) to embrace the latest best practices and security features in a comprehensive, holistic matter.

This white paper is an attempt to help you do just that. Our goal in writing this white paper is to provide you with an overview of industry best practices and available fraud controls to help you mitigate risk in a faster payments world. With this as our objective, we paint a picture of the faster payments landscape, give you an overview of industry stakeholders and players, outline faster payments risks and vulnerabilities, and introduce cutting-edge tools and strategies for securing faster payments.

Let’s begin with an overview of today’s faster payments landscape.
The Faster Payments Landscape

Faster payments are on the rise, and with this, the potential for increased fraud. A cursory review of the past few years reveals we have moved beyond conceptualizing faster payments to implementing them. With that shift, it is more important than ever that we remain vigilant in ensuring our payments system remains safe and secure.

Here are highlights from the past few years.

NACHA was an early starter in the race to faster payments, launching Same Day ACH Phase 1 (credit entries with funds available at the end of RDFI processing day) on Sept. 23, 2016. The rollout was near seamless, although rumblings about a potential uptick in fraud were heard long before Phase 2 (credit and debit entries with funds available at the end of RDFI processing day) rolled out on Sept. 15, 2017. Despite predictions of rising fraud, initial reports are encouraging. NACHA’s Same Day ACH Survey, conducted in November/December 2017, reported for the fourth consecutive time “not one respondent saw any increase in fraud due to Same Day ACH.” Phase 3 (credit and debit entries with funds available by 5 p.m. RDFI local time) went into effect on March 16, 2018. According to NACHA, the future for Same Day ACH as a safe, secure way to move money faster looks bright.

Another early player was Zelle, a new person-to-person (P2P) payments network from bank-owned Early Warning Services. Zelle went live in June 2017 and exploded. Recent reports indicate that Zelle moved a record $75 billion in 2017—a remarkable feat by most accounts.

Close on its heels, The Clearing House’s (TCH) RTP® System launched in November 2017. RTP is the first new core payments infrastructure in the U.S. in more than 40 years. According to a Nov. 14, 2017, press release, “The new RTP system was designed and built through the collaborative effort of TCH’s 25 owner banks and meets the objectives of the Federal Reserve Faster Payments Task Force. RTP is open to all U.S. depository institutions with a goal of reaching ubiquity by 2020.”

This says nothing of the many other forms of faster payments, most of which focus on P2P transactions, that went to market in the past few years — Apple Pay, Samsung Pay, Ripple and bitcoin to name just a few. Currently, we are seeing momentum around B2B faster payments, and expect new developments in the future.

These faster payments initiatives launched against the backdrop of the Federal Reserve’s Faster Payments Task Force (2015-2017), which included a diverse array of stakeholders in advancing the work outlined in Strategies for Improving the U.S. Payments System (PDF). The task force completed their work in 2017, calling on all payments stakeholders to embrace their plan,
described in Final Report 1 and Final Report 2, and vision for secure, ubiquitous, faster payments by 2020.

Established in June 2015 in support of Strategies for Improving the U.S. Payments System, the Federal Reserve’s Secure Payments Task Force ran concurrently with the Faster Payments Task Force. The Secure Payments Task Force concludes its work in March 2018. As noted on its website, its mission in part is to “provide a forum for stakeholders to advise the Federal Reserve in its leader/catalyst and operator roles on payments security matters.” Task Force participants will continue their work, transitioning into the Federal Reserve’s FedPayments Improvement Community.

As is evident, the rate of industry change over the past few years in the area of faster payments is unparalleled. Unique to this movement is the level of collaboration among industry participants in working together to not only move payments faster but to also keep them safe and secure.

Raise the topic of faster payments, and it won’t be long before someone brings up the issue of faster fraud. And it’s true. With shorter processing and settlement windows and payments that are irrevocable, opportunities for faster fraud abound.

Let’s take a closer look at the industry’s key players and stakeholders.

Key Industry Players

NACHA

NACHA was an early adopter of faster payments with its introduction of Same Day ACH (SDA), which enabled the same day processing and settlement of virtually any ACH payment. In rolling out Same Day ACH, NACHA opted for a phased approach to implementation. To reiterate:

- Phase 1 went into effect on Sep. 23, 2016 (credit entries with funds available at the end of RDFI processing day).
- Phase 2 went into effect on Sept. 15, 2017 (credit and debit entries with funds available at the end of the RDFI processing day).
- Phase 3 went into effect on March 16, 2018 (credit and debit entries with funds available at 5 p.m. RDFI local time).

Despite widespread speculation about increased fraud, NACHA, in a news release dated Jan. 16, 2018, stated that a survey revealed no financial institutions reported an increase in fraud due to Same Day ACH (SDA) despite increasing SDA volume. The survey, conducted in November/December 2017, included 22 financial institutions that represent 78 percent of ACH Network origination volume. This finding is consistent with previous surveys conducted in December 2016/January 2017, March/April 2017, and September 2017.
More recent numbers pulled from the February 2018 *Same Day ACH Corporate Survey* conducted by NACHA and PYMNTS.com found no connection between SDA products and increased fraud for more than 92 percent of financial institutions surveyed. Furthermore, nearly 91 percent of corporations with revenues greater than $50 million and more than 93 percent with revenues below $50 million reported having no issues with fraud and SDA.

While this news is certainly encouraging, keep in mind that fraudsters are always on the prowl. While it is important to put fraud controls in place, it’s equally important to regularly monitor your systems and processes and make necessary changes and adaptations along the way.

**The Clearing House**

On Nov. 13, 2017, The Clearing House (TCH) launched RTP®, its real-time payments system—the first new core payments infrastructure in the U.S. in more than 40 years. The new RTP system meets the objectives of the Federal Reserve Faster Payments Task Force and is open to all U.S. depository institutions. Its goal is to reach ubiquity by 2020, the same objective set by the Federal Reserve’s Faster Payments Task Force.

Tim Mills, AAP, Vice President of RTP Business Development for The Clearing House Payments Company, explains it this way:

*RTP is a payments infrastructure much like a computer’s operating system. From a risk perspective, it is a platform designed to address traditional risk issues safely. For example, credit push removes risks associated with legacy debit models. RTP also uses a prefunded settlement model, which ensures funds are available before settlement occurs, and a centralized risk engine uses historical activity to reduce future risks associated with transactions. RTP’s legal framework puts a great deal of responsibility on the institution that is sending payment to put appropriate controls in place.*

The greatest takeaway from this statement is simply this: *It is incumbent upon the financial institution that is sending payment to put appropriate controls in place.*
The Federal Reserve

The Federal Reserve recognizes that the payments system stands at a critical juncture in its evolution. And why wouldn’t it?

Technology is changing the payments landscape, high-speed data networks are everywhere, computing devices are growing more sophisticated and mobile, and information is increasingly sent and received in real-time, which is contributing to end-user expectations for payments services.

From where we sit, fraudsters are growing savvier by the day, and the sophisticated level of fraudulent attempts on payments is at an all-time high. We spoke with Phil Ridgway with the Retail Payment Office for the Federal Reserve Bank of Atlanta, whose responsibilities include fraud management and risk mitigation, and he agreed, underscoring that payments systems today face dynamic, persistent and rapidly escalating threats.

To help combat these threats, Ridgway said the Fed is seeking input from industry stakeholders:

> The Retail Product Office is continually pursuing system improvements, such as our ACH Modernization efforts, which will facilitate new services and enhancements to existing services in support of faster ACH. We actively seek feedback from our customers to help us define these future capabilities, and would encourage customers to leverage their Account Executives as a means to provide any comments or suggestions.

Recognizing the importance of governance through rulemaking in the fight against fraud, the Federal Reserve Bank implemented both Phase 1 and Phase 2 of NACHA’s Same Day ACH rule change. Most recently, Phase 3 went live in March of 2018 with the Federal Reserve’s support.

Adopting these rules affords the secure movement of payments between parties and ensures transparency in such key issues as timing, fees, error resolution, liability and more.

In discussing the Federal Reserve, it is important to note that the Fed made and continues to make significant contributions to moving faster payments forward. Its work through the Faster Payments Task Force and the Secure Payments Task Force embodies the organization’s commitment and contribution to securing faster payments. In pursuit of its goal to realize a vision for a payments system in the U.S. that is “faster, ubiquitous, broadly inclusive, safe, highly secure and efficient by 2020,” the Faster Payments Task Force created a guiding document, *The Faster Payments Effectiveness Criteria*. This seminal work serves as a roadmap for the future and will shape the industry for years to come.

Its work completed, the Faster Payments Task Force disbanded in late 2017. Many of the initiatives begun by the task force live on through workgroups and other industry initiatives.

The Secure Payments Task Force is experiencing a similar fate, concluding its efforts in March with a final publication consisting of a collection of educational materials outlining the lifecycles and security profiles of today’s primary payment methods.
According to a March 1, 2018 press release distributed by the Federal Reserve, “[Secure Payments] Task Force participants will transition into the Federal Reserve’s FedPayments Improvement Community, established to provide stakeholders with opportunities to engage in the Federal Reserve’s ongoing payment improvement initiatives.”

More information about the Fed’s role in faster payments is available at www.fedpaymentsimprovement.org, including the Fed’s Strategies for Improving the U.S. Payments System.

Other Players Shaping the Industry

Traditional service players are not the only ones shaping the faster payments landscape. Cutting-edge technology, combined with forward-thinking, innovative solutions, has put fintechs front and center in the race to faster payments, especially in the area of P2P payments.

Fintechs, businesses that provide financial services using technology, both compete and collaborate directly with financial institutions, selling innovative products and solutions to FIs as well as their customers or members. Fintechs hold a broad appeal to millennials and subsequent generations that prefer simple, quick and digital financial services.

The following fintechs, most of which are focusing on P2P payments, are making their mark in the world of faster payments.

On Sept. 9, 2014, Apple® announced the release of ApplePay™, which they describe in a press release as “a new category of service that will transform mobile payments with an easy, secure and private way to pay.” Despite high hopes and early hype, ApplePay is still struggling to gain traction and by many reports has underperformed.

Then there is Samsung Pay, the company’s answer to ApplePay, which launched on Sept. 28, 2015. Unlike other systems, Samsung Pay uses what’s known as “tokenization.” When you make a payment, rather than your credit card information going to a terminal, your phone uses a temporary number that the credit card company provides. Its intent is to provide a more secure way of generating payments, making the customer’s information less vulnerable to theft. Samsung Rewards, a tiered system that awards users for using their mobile wallet, is what distinguishes Samsung from its competitors. Although it is too early to say how it will fare in the long run, Samsung Pay is experiencing robust, initial success with its mobile wallet.

Venmo is another relatively new player. A mobile payment service founded in 2009 and owned by PayPal, Venmo, unlike other digital wallets, is a social network in itself and is particularly appealing to urban millennials. In 2016 alone, Venmo handled $17.6 billion in transactions.

Of course, other players and technologies are shaping the industry, including Ripple, which focuses more on global payments, blockchain, which is a public ledger of cryptocurrency transactions, and others.

Now that we have identified the key industry players, let’s examine faster payments risk and vulnerabilities.
Faster Payments Risk and Vulnerabilities

According to some experts, faster payments naturally equate to faster fraud. They point out that fraud tripled in the United Kingdom in the wake of faster payments and postulate that the U.S. should expect a similar fate.

While it is impossible to thwart every faster payments fraud attempt, it is unlikely the U.S. will see the same escalation in fraud the U.K. did, simply because we have more advanced fraud tools and resources available today, which we will discuss later in this paper.

Still, it is essential to understand what makes faster payments so appealing to fraudsters and recognize vulnerabilities.

First, the many legacy systems in place at today’s financial institutions are not equipped to ferret out fraud that moves at the speed of payments. Financial institutions still rely on manual processes that are of little use when it comes to faster payments. Without the implementation of new controls designed to manage and mitigate faster payments fraud, loss and reputational damage are likely to rise as payments move and settle faster.

Another obstacle to overcome is siloed processes and single-point solutions that don’t “talk to each other.” This siloed mindset transfers into many areas of the business model. For example, most financial systems are relying on their own data rather than undergirding their discoveries by tapping into data outside of their four walls. This limited view of potentially fraudulent activity increases an FI’s risk exposure.
Operational Risk

When talking about faster payments, operational risk is front and center. Let’s begin by defining operations and operational risk in the context of our discussion. Operations refer to the people, processes and systems in place that facilitate the movement of payments. Thus, operational risk relates to vulnerabilities specific to these areas that fraudsters can exploit.

For example, in the case of Same Day ACH, shortened settlement windows give fraudsters the opportunity to bypass manual fraud prevention tools. Also, the addition of two new clearing windows affects internal processing schedules and systems, settlement times and dates, cut-off times and downstream operations and processes—all of which increase operational risk.

From an operational perspective, when it comes to real-time payments, the window for catching fraud is even smaller. To further complicate matters, once an individual or organization sends a payment, that payment is irrevocable. Real-time payments require innovative technology and products designed to alert financial institutions to potential fraud and, specifically, to stop real-time fraud as it happens. Without it, financial institutions, payments processors and their customers or members face potential financial and reputational loss.

Operational risk is complex and multi-layered, and when it comes to putting controls in place to address it, there is no one-size-fits-all solution. It is the responsibility of the financial institution to work closely with a provider to determine which solution(s) meet the unique needs of its organization.

For your convenience, we are providing a list of third-party processors at the end of this paper to help you find a solution that meets the needs of your organizations.

Cyber Risk

Cyber risk might be the most significant risk facing financial institutions today. Cyber risk refers to the degree of damage, loss or disruption due to an information technology system failure.

Let’s unpack this with an illustration.

Consider the 2015-2016 cybersecurity threats against SWIFT. (To learn more about the attacks, read The New York Times article, “Once Again, Thieves Enter SWIFT Financial Network and Steal.”) These attacks were a watershed moment for the industry as SWIFT is widely thought to be the most secure financial messaging system in the world. As the article in the Times reported, “It is as if the thieves used their hacking skills to reach inside a bank vault.”

In its article, “Cybercriminals versus Financial Institutions in 2018: What to Expect,” another online news source SecureList speaks to cyber risk:

In 2017, we saw the range of financial organizations that cybercriminals have been trying to penetrate expand significantly. Different cybercriminal groups infiltrated bank infrastructure, e-money systems, cryptocurrency exchanges, capital management funds and even casinos. Their primary goal was to withdraw vast sums of money.
A November 2017 article, “Threat Predictions for Financial Services and Fraud in 2018,” goes further, offering this explanation:

Customer data is a crucial enabler for large-scale fraud attacks and the frequency of data breaches among other successful attack types has provided cybercriminals with valuable sources of personal information to use in account takeover or false identity attacks. These account-centric attacks can result in many other losses, including that of further customer data and trust, so mitigation is as essential as ever for businesses and financial services customers alike.

When it comes to faster payments, cyber risk heightens as a point of concern. It takes advantage of the points of entry into the payments system—computer systems, credentials, individual phishing efforts, etc. Couple that with a faster payments environment where there is less time for detection via standard controls, and you have the potential for serious fraudulent activity.

Jane Hennessy, Head of External Alliances for G2 Web Services, speaks to a different type of fraud, one we often overlook. She points out some financial institutions think the way to shut down faster payments fraud is to avoid faster payments altogether. This, too, puts financial institutions at risk. “Financial institutions not offering faster payments risk losing market share, customers or members to their competitors,” says Hennessy. “If your customer finds a service they are looking for at another institution, that institution will do all that it can to gain the customer’s remaining business.” That’s a risk you can’t afford to take.

While an in-depth look at all of the various types of faster payments fraud is outside the scope of this paper, it is vital that financial institutions educate themselves about other types of fraud (reputational risk, compliance risk, know-your-customer risk, etc.) and find ways to stop it.
Securing Faster Payments

Operational risk. Cyber risk. Reputational risk. What’s a financial institution to do?

Frankly, this question is difficult to answer, since at this juncture we have very little data on faster payments fraud. Of course, our “tried and true” risk resources still exist—multi-factor authentication, dual-control, positive pay, debit blocks and more. But in today’s faster payments world, these systems—though still effective in many instances—require augmenting for faster payments.

After speaking with various payments risk experts and thought leaders, we’ve come up with what we believe are best practices for fighting faster payments fraud. Keep in mind because the industry is rapidly evolving, so are the solutions aimed at combatting fraud. However, our goal is to provide a starting point upon which you can build as faster payments develop and fraud solutions evolve with it.

We begin with an overview of FedACH Services.

FedACH Services

According to the Federal Reserve’s website, FedACH® SameDay Service “enables processing, editing, distribution and settlement of virtually any ACH payment during the current processing day as provided for in the ACH Rules.” Also, the ACH Rules exclude from eligibility international transactions (IAT), automated enrollment entries (ENR), and transactions above $25,000. Additionally, to process and settle same day transmission deadline and not contain a future date in the effective entry date field.

Other risk mitigation tools, as noted on the Fed’s website, include:

- **FedACH Risk® Origination Monitoring Services**: This service allows ODFIs to monitor ACH batches associated with selected routing transit numbers (RTNs) and company IDs. Financial institutions can tailor and self-administer the monitoring criteria to reflect their particular risk management strategies and customer profiles. Benefits include monitoring accumulated totals over a single processing day or across multiple exposure days, generating a variety of monitoring reports, including criteria summary reports, historical management criteria, origination monitoring event reports, and more.

- **FedACH Risk RDFI Alert System**: This service provides notice of unusual or noteworthy conditions within a Receiving Depository Financial Institution’s (RDFI) incoming FedACH Service batches and files and the RDFI account holder’s incoming items. It helps alert the RDFI and its account holders to potential fraud attempts, significant origination errors, situations requiring further action, etc. The RDFI Alert System allows FIs to take prompt action in a faster payments environment.
FedPayments® Reporter Service: This service enables financial institutions to automatically search Automated Clearing House (ACH) files for valuable ACH information—such as return items, DNE entries, IAT transactions and financial EDI messages—convert this data into human-readable reports, and distribute this information within an institution and out to its business customers or members. Depository institutions can use this information to identify Same Day activity and trends.

These services are available for both RDFIs and RDFI customers or members, which are typically business customers. Here’s how Ridgway describes the services:

- Risk Origination Monitoring provides a means to monitor the activity of either the ODFI or a Corporate Customer of the RDFI. The service will pend work (and send an email notification to the DFI) that meets any dollar value caps configured by the DFI, which effectively stops its processing until either the DFI reviews the work and decides to release or reject it or the DFI allows their configured end-of-day defaults to automatically decision the work. Any work that pend in the Risk Origination Monitoring received before the final Same Day deadline, will only qualify for Same Day processing if an individual enters the information manually before the final Same Day deadline. This may have an advantage for DFIs that wish to manage select Same Day originators as a means to avoid inadvertent Same Day origination.

- FedACH Risk Origination Monitoring also has a Company ID Inclusive option, which means the Fed would pend any batches that come in from a Company ID that has not been identified by the ODFI. The service monitors work by RTN, whether the files are sent by the ODFI or by its service provider, so it adds fraud review capabilities even for outsourced DIs.

- ACH Risk RDFI Alerts provide file and batch notifications that meet customer-defined criteria go to the receiver after each file distribution; item alerts release at the end of the processing day. RDFIs may utilize the batch alerting to receive notifications of Same Day batches after each file distribution and Same Day items at the end of the processing day. Further, RDFIs may set criteria to receive notification of all Same Day work or just work that meets specific criteria for ODFI, Company ID, SEC, item/addenda count, or dollar value.

- The FedPayments Reporter product can analyze Same Day ACH activity for either the DFI or the customer of the DFI through its Originated Batch Report, Received Entries Report, Return Item Report and Return Ratio Report. Also, these reports may help to facilitate internal analysis of customer usage of the Same Day service and as a means to establish new Risk Origination Monitoring or RDFI Alerting criteria.

To learn more about these resources, visit the Fed’s Risk Management Toolbox: https://www.frbservices.org/resources/resource-centers/risk-mgmt-toolbox/index.html.
Onboarding and Monitoring

While the Federal Reserve offers specific services to support fraud mitigation, we believe the right due diligence of your customers or members at the upfront can have a profound impact. The challenge lies in balancing a robust onboarding process with a positive customer experience that does not result in abandoning the enrollment process because of too much friction.

Over the past five to seven years, synthetic identities have risen exponentially. Synthetic identities are a fictional identity created by combining real, often stolen and fake information to create a false identity. The criminal then uses the synthetic identity to open new accounts and make unauthorized purchases. Often the fraudster uses the social security number of a child or someone who is deceased to create a false identity and engage in criminal activity.

In addition, it is not uncommon to create what appears to be a legitimate business account only to find out the business is a front for illegal drug activity or prostitution. Fraud causes millions of dollars in loss each year, and that number will rise exponentially unless financial institutions put proper controls in place. But what constitutes an effective onboarding process?

Audrey Touma, Senior VP Product, GIACT, a company focused on real-time payment risk and fraud solutions, urges financial institutions to ask themselves these important questions when onboarding potential new customers or members:

- Does the customer’s information check out? Are they who they say they are?
- Is data, social security number, date of birth or any other PII information misaligned?
- Does this person have prior information or associations?
- Can you validate an email or social media presence?

Perhaps one of the biggest mistakes financial institutions make when it comes to onboarding new customers or members is relying on siloed information available directly to the bank rather than seeking outside data sources to validate the application data of a customer.

To mitigate faster payments fraud, financial institutions should work in their strengths and recognize when the support of a reputable third-party processor or other supplemental source could simplify the process and catch anomalies in the enrollment process before fraud occurs.

The old axiom, “If at first you don’t succeed, try, try again,” holds a lot of truth when it comes to faster payments fraudsters and the onboarding process. Fraudsters will try multiple times and ways to create new accounts, which is why continual monitoring of new customer applications and customer accounts is critical to success.
A Word about Third-Party Processors

It is imperative to pursue due diligence and exercise good business sense when onboarding vendors because increasing the number of vendors can also increase the potential for fraud. And the bottom line is this—the liability is yours. You are responsible for vetting your third-party processors and also knowing what relationships they have. It’s the “know your customer” and “know your customer’s customer” applied to third parties.

You can significantly reduce the likelihood of this happening by knowing from the start what you are trying to accomplish. Once you identify the problem you are trying to solve, you can choose a specific vendor or vendors that meet your criteria rather than onboarding several.

Behavior Analytics

From the historical recommendation of meticulous onboarding, we move to evaluate an emerging fraud solution: behavior analytics. Simply put, behavior analytics is data gathered on how customers or members behave. Often what we do is a better indicator of who we are than who we say we are, which is a common authentication question. For example, our purchasing habits reveal a great deal about who we are—where we shop, how much we spend, what time of day we make purchases, the types of establishments we frequent, and the goods we buy. Other behaviors monitored include:

- How much money we usually keep in our account
- Average purchase price for an item
- Withdrawal amounts
- Location of user/transaction
- Number of login attempts
- Unusual behavior, activities, or purchases

Financial institutions, using behavioral analytics, can flag actions inconsistent with previous patterns and purchases, which help in determining when someone is using your information to make a purchase. Financial institutions are already employing this control for credit and debit card fraud, so the industry has a model and a precedent to draw from in applying this method to customer accounts as it relates to faster payments.

Monitoring a customer’s behavior in a world of real-time payments requires technology that can identify anomalies almost instantly and put a hold on a customer’s account until the institution verifies the customer’s purchase. As someone once said, “Your fraud technology needs to keep up with the speed of payments.”
Transactional Analytics

Transactional analytics keep track of customers’ or members’ payments activity, noting average payment or debit amount, types of payments, average balances, etc. Appropriate fraud controls flag questionable transactions.

For example, if Customer A’s account shows regular debits made for payroll, vendor services, and travel, etc., a large dollar debit in the amount of $24,000 coming in via Same Day ACH and going out to a questionable overseas organization at the end of the day should raise a red flag. Ideally, your software or vendor partner would put a hold on the transaction or deny it until it received confirmation from the customer that it is a legitimate debit.

When analyzing transactions, keep in mind that fraudsters sometimes wait as long as six months after opening an account to perpetrate fraud. To protect customer accounts, financial institutions should consider such account controls as setting appropriate exposure limits, limiting initial funding dollar amounts and methods, as well as others.

Remember, when working with real-time payments, once an individual or institution sends a payment, it is irrevocable. It is critical that real-time payments have real-time fraud controls in place.

Software as a Service

In their efforts to combat fraud and save money, many financial institutions opt for SAAS or Software as a Service as a stopgap measure. However, going this route can give rise to multiple problems, e.g., the software isn’t compatible with the core of the financial institution’s internal network, inflexibility of many programs, and the inability of financial institutions to customize the rules that would raise a red flag, leading to false positives and irritated customers or members.

When evaluating real-time fraud software, consider looking for these essential features:

- Detects fraud in real-time or near real-time
- Uses various analytics
- Enables the financial institution to alter the rules to include:
  - Automated responses, including an automatic return
  - Immediate responses, such as deny, suspend, etc.
- Creates a trail for auditors

Again, should your financial institution decide to use SAAS software, you should practice due diligence, making sure you know what you are purchasing.

Service Suites

The sophistication of today’s fraudsters, coupled with shorter windows to identify fraudulent attempts due to the faster movement of money, sometimes makes partnering with one vendor that offers a suite of services a better option than working with multiple vendors for multiple solutions.

Before partnering with any solution provider, do your homework. Make sure the suite of services you are purchasing include such offerings as confirming an individual or business’ identity, ensuring compliance requirements are met, before ascertaining funds availability, and other options that would support your organization in mitigating fraud.

It is up to you to determine whether an individual faster payments fraud mitigation solution or a suite of services would best meet your needs.
Next Steps for Financial Institutions

As you consider your individual faster payments strategy and explore fraud mitigation options, remember this is a new market and more products and services are on the horizon. Every financial institution needs to determine what it is trying to accomplish, assess its risk tolerance, and decide on a course of action to support where it is today and where it wants to go in the future.

So, where do you begin? We recommend considering the following issues when creating your faster payments security strategy:

1. Determine where your risk lies as relates to your faster payments strategy. Not every solution is right for every financial institution, and you may want to prioritize implementation of certain preventative measures based on the aggressiveness of your strategy.

2. Identify where your institution is now in relation to current processes and products, along with your existing risk management strategy. Do your existing products and processes have real-time capabilities? Will your existing processes and products take you where you want to go?

3. What next steps do you need to take toward educating yourself about available faster payment controls and options?

4. What additional tools, resources and information do you need before making a decision?

5. How can you help educate and build consensus among decision-makers in your organization?

6. Consider, too, the risk of adopting a “wait-and-see” approach and choosing not to engage in faster payments. Weigh the cost of adopting faster payments against the cost of doing nothing.

While these general guidelines are a helpful place to start, they are no substitutes for seeking individualized guidance and input from a payments risk specialist. We invite you to reach out to a member of the NEACH staff or a payments risk expert for individualized support. For your convenience, we have included a list of solution providers on the following page.
Summary

Significant changes are happening in the world of faster payments. As an industry, we are in a time of transition—faster payments are exploding, and with it, the potential for faster fraud.

Wondering what next steps to take? Consider contacting one of these solution providers to learn more about available fraud mitigation and security solutions.

Solution Providers

**Federal Reserve**
Risk Management Toolbox
FedACH and Check Services Customer Support
1-877-372-2457

**Fiserv**
Risk, Fraud & Compliance
1-800-872-7882

**G2 Web Services**
Risk Management Solutions
1-888-788-5353

**Giact**
Risk, Compliance & Fraud
1-866-918-2409

**RP Payments Risk Consulting Services**
Payments Strategy and Risk Advisory Services
1-816-204-1846

**RSA**
Fraud Prevention
1-800-995-5095

**Tyfone, Inc.**
Banking that is Convenient, Secure, and Omni Channel
503-226-3939

We cannot emphasize this point enough—it is the responsibility of the financial institution to put appropriate fraud controls in place. While there is a cost associated with purchasing new technology and tools, there is also a cost for not engaging in faster payments. In light of the faster payments trajectory we’ve seen over the past few years, we believe the cost of not acting is more than any financial institution can afford.

We hope you will use the information and best practices outlined in this white paper to take strategic action, create a faster payments risk mitigation strategy, and implement it across your organization.

Consider NEACH your faster payments partner. We invite you to reach out and let us know how we can help.

Summary
About NEACH

NEACH is a non-profit trade association with more than 40 years of experience helping members originate and receive ACH transactions. NEACH provides products, services, education and marketing to its member institutions and other New England entities to increase the acceptance, use and quality of electronic transactions.

www.neach.org