Managing Risk in Real Time:
The changing payments landscape, Real Time Payments, and risk

The payments landscape in the U.S. has always been changing—technology upgrades, shifts in usage, etc. But now it’s **really** changing. In little more than a decade, we’ve seen financial services go digital and then mobile, while fintech providers flood the playing field. We’ve seen big spikes in usage (ACH racked up over $6B in transactions during Q2 2019, up almost 8 percent from Q2 2018), including big increases in faster payment methods (Same Day ACH jumped 46 percent over the same period, accounting for nearly $60M in transactions). And we’re on the verge of widespread adoption of a new generation of real-time payment options.

It’s a lot to keep up with, and a lot to manage in terms of risk.

In this report, we’ll take a look at existing and emerging solutions, explore the unfolding future of the marketplace, and discuss the risks involved in payments—as well as how to manage them in this constantly evolving landscape.
Part I: A state of constant change

Want to feel old? Find a nineteen-year-old and tell them, “I remember when it took days for a transaction to process.” In the time it takes to make that member of Generation Z wrinkle their forehead in disbelief, countless transactions are being fully processed—and payments are on the verge of getting even faster for far more users.

This change is due in large part to mobile technology and the ease with which developers can make new services—financial and otherwise—available at scale. We’ve seen an explosion of single solution mobile apps that offer payment solutions, financial management tools, and more.

Single solutions and consumer payments

A crowded market

When we talk about the state of change in the payments space, we’re most often talking about consumer payments—and for good reason. In the last decade, we’ve seen fintech providers with consumer offerings appear at an incredible rate. In the payments space alone, there are 600+ companies competing for shares,1 with most consumers using multiple solutions to make payments to billers, vendors, and individuals. It’s fairly typical for the average household to make e-commerce purchases via debit or credit cards, PayPal, or an app like Apple Pay or Google Pay, while paying their bills via billers’ websites or their financial institution’s (FI’s) bill pay tools.

More payments = more risk

New solutions bring new risks—many of them unknown to the average consumer. While compliance requirements and reputational concerns compel FIs to manage a great deal of risk, many fintech providers’ concerns with reducing friction at all costs leaves their applications and users open to risk. For example, according to Consumer Reports, some of the most popular P2P (person-to-person) payments apps have problematic data privacy and data security operations/policies. And some have default security measures that require no authentication (i.e., a password, fingerprint, or PIN) to initiate transactions.2

While some of this risk can be mitigated through best security practices—such as making default app settings require authentication—some risk is simply baked into the presence of financial data and access points on mobile devices. Losing your phone is equivalent to losing your wallet.

Some providers will weather security and compliance issues better than others but, again, employing best practices will help—as will having the right tools. Technology like machine learning, behavioral analytics, end-point interrogation, and multi-factor authentication will all play a part in maintaining security and managing risk.

Financial institutions have been managing all of this for decades and have regulatory requirements that ensure they address certain kinds of risk. The risk related to payments is new to a lot of fintech
providers, though, and often outside their area of expertise. They’ll need to either purchase solutions applicable to their risk, or partner with organizations that have an existing scalable security infrastructure. We’re seeing the latter occur more and more frequently as fintechs and FIs are both becoming more amenable to partnering, rather than seeing one another as competitors.

FIs and Fintechs: From Competitors to Partners

FIs and fintechs have very different approaches, strengths, and needs when it comes to offering payments solutions.

**Financial Institutions**
- Have been doing this a long time
- Provide robust infrastructure and user base
- Have compliance baked in to their business model
- Are equipped with tools and strategies for managing risk

**Fintech developers**
- Know how to build amazing experiences
- Are more likely to embrace new strategies and business models
- Don’t have the same compliance requirements (which can expose them and their users to risk)
- May be completely new to security concerns and dependent on third-party assistance

For years, these two verticals considered each other rivals, but that’s rapidly changing. By partnering, FIs and fintech providers can together offer best-in-class experiences while ensuring compliance, mitigating risk, and ensuring more secure transactions. **Both can embrace the best of both worlds to their benefit—as can their users.**

Fewer competitors for commercial payments

The noise level in the commercial payments arena is lower. In the consumer realm, we’re seeing a wide array of emerging methods—including Zelle, Venmo, Google Wallet, and Square Cash. We’re also seeing countless brands—from ExxonMobile, Gulf, and Phillips 66 to Starbucks, Target, Wal-Mart, and Dunkin Donuts—developing mobile wallets. But in the commercial arena, we’re only seeing a handful of these newer options making inroads—including Venmo and Zelle, though they’re affecting commercial payments practices to a much smaller extent than they’re impacting consumer payments.

All of this said, these fintech-flavored changes are just the tip of the iceberg. A much bigger transformation is underway.
Part II: The transformation

The mobile age has introduced a new transactional model. The drive-to-the-store-and-wait-in-line way of doing things still exists, but consumers and businesses both want faster options. Expectations have changed and the industry has responded with a number of ways to make faster payments.

**Same Day ACH**

While they don’t quite take place in real time, NACHA’s Same Day ACH transactions are measured in hours rather than days—and they’re widely available, with roughly 99 percent of ACH transactions eligible for same-day processing. A notable downside is that Same Day ACH does come at a cost. While FIs can recoup that expense by charging for same-day service, this, along with its not-quite-real-time speed, puts Same Day ACH at a disadvantage when compared to other real-time options we’ll discuss shortly.

That said, Same Day ACH is flourishing. Just three years after its introduction, Same Day ACH is responsible for $50+ million in transactions per quarter.

**Credit Push Payments**

Historically, a large number of transactions have been “pull” payments, meaning that they’ve been drawn from the payer by the payee, using information supplied by the payer to the payee. Push payments flip this model; the same rails are used, but the payment is pushed from the sender to the recipient. This model has some clear advantages. Because the payment is pushed from the card or bank account of the payer through their core/card processor their card/account information isn’t sent directly to the payee—and isn’t therefore put at risk. Of course it’s always possible for card information to be compromised (by phishing, etc.) but it’s less likely that a bad actor would be able to insert themselves into a credit-push transaction.

On the downside, the push model is a fairly open system between various card processors, payment providers, etc. This means it depends on database directories of user information to carry out transactions. Any lag in the maintenance of these directories could introduce risk. If, for example, a user changes FIs or opens a new account and the directory isn’t updated in a timely manner, payments may be delivered to the wrong account. Liability in this case could fall on the sender or receiver’s FI, the processors used by the FI, or possibly even the consumer.
New Rails: Access and Expectations

While fast, innovative, and remarkable in their own right, the above applications and approaches all rely on existing payment rails. But the biggest change to date is the emergence of the first entirely new set of payment rails in the U.S. since the creation of ACH more than 40 years ago.

This new platform, The Clearing House’s RTP® (Real Time Payments) platform is available to all federally insured U.S. depository institutions. There is, however, some controversy about The Clearing House’s ability to make the platform fully available to all FIs. Because The Clearing House is owned by two dozen of the largest FIs in the country, smaller FIs in particular are concerned.

The Clearing House has stated that it intends to reach ubiquity—being available to over 11,000 FIs nationwide—by 2020. And they have boasted that the RTP network now reaches over 50 percent of U.S. deposit accounts—but this percentage is misleading, as it reflects more about the size of the FIs currently using the network than the number of FIs on it. In fact, as of late 2018/early 2019, only 11 of the 24 Clearing House owner-banks had successfully implemented the system.

Globally speaking, this kind of comprehensive real-time rail system is nothing new. Since the launch of Japan’s Zengin System in 1973, roughly 40 countries have put real-time platforms in place.

Nor, in the days ahead, will The Clearing House’s RTP be a unique offering within the U.S.; the Federal Reserve, after lengthy deliberation, has recently announced plans to launch a real-time rail option of their own called FedNow.

Some critics of a second real-time system are quick to point out that the Monetary Control Act prohibits the Fed from creating systems unless they’re impossible for the private sector to build. But there’s a reasonable case to be made for the platform. Private solutions are, by nature, closed systems, limiting real-time payments to the network of users included in the system. The Fed overcomes this limitation with its already-established connection to all the existing FIs in the U.S. This scale and The Fed’s promise of universal access are important points, as those most heavily impacted by delays in payments are low-income individuals living paycheck to paycheck and small businesses in need of predictable cash flow.

The details of FedNow’s rollout and its ultimate impact remain to be seen, as it isn’t likely to launch until 2023 at the earliest.

Reducing risk and creating conversations

The Clearing House’s RTP is a credit-push-based system, giving it a different risk profile than ACH transactions, including Same Day ACH. This model puts the FI’s customer in control—they instruct the FI to initiate payments; there’s no third-party authorization—and it’s a simpler design, with fewer moving parts. This limits the scope of cyberattack, as criminals must crack one account at a time.

RTP At-a-Glance

- Credit Push
- Immediate Confirmation
- Payment Certainty
- Funds Immediately Available
- Full Accounts Receivable/Payable Messaging
- Data Extensibility
- Multiple Case Uses
- Global Ready
For consumers, the need for real-time payments comes down to user expectations. They’re carrying out commerce with the expectation of immediacy. A click or a swipe completes transactions as far as modern users are concerned; they don’t want to worry about returns, delays, or fees related to funds not being accessible at the right time.

While speed matters for businesses as well, RTP’s biggest benefit for commercial users is the ability to include remittance information with the payments. The ability to include a conversational element within the payments process has long been missing, and RTP has the ability to remedy this.

See Fig. 1 below to see how a “conversation” can be built into payer/payee transactions with RTP.

**Fig. 1 – RTP’s Transaction Conversation**
Part III. Managing Risk

Transaction volume is a huge factor when weighing risk. The ability to monitor for fraud at scale is crucial in controlling FIs’ exposure to risk. ACH and Same Day ACH transactions have both seen incredible growth in the last few years. As RTP and FedNow add to the mix, we’ll likely see even more volume—and at greater speeds. This is problematic. Traditional ACH payments allowed several days for FIs to detect and investigate suspicious activity. Same Day ACH reduced this window to as little as two and a half hours and increased the movement of funds from once daily to three times per day. Even if FIs could handle the increased volume or the increased transaction speeds individually, putting the two together is a surefire recipe for risk.

While RTP further reduces the window for fraud detection to seconds, it’s important to remember that, as a credit-push system, it presents a different risk profile than payment methods like check and ACH. For RTP, managing risk will be more a matter of verifying that, when users initiate transactions, the payments are going to the correct party. In this sense, RTP is more similar to wire, where a large part of managing risk is teaching users to recognize fraudulent requests from criminals pretending to be valid requesters.

5 Musts for Managing Risk

Risk encompasses a lot, as does risk management. But embracing just a handful of fairly simple strategies can help reduce the risk presented by the ever-changing technology, tools, and timeframes involved in payments.

1. Automation is a must

We’ve already touched on some of the risks posed by the changing payments landscape; one in particular bears repeating: more payments = more risk. The number of transactions processed hourly—much less daily—has grown too high to monitor manually. Automation is mandatory—literally. The Clearing House has mandated that institutions participating in RTP must have automated solutions for monitoring transactions. Fortunately, the last decade has seen the development of highly sophisticated, real-time solutions that employ behavioral data and machine learning to monitor transactions and detect suspicious transactions. You’ll also want a comprehensive positive pay system that can help both your back office and your teller line recognize potentially fraudulent ACH transactions and checks.
2. **Don’t let disputes overwhelm your back office**

Not only do payment providers need a way to mitigate risk through fraud detection, but they also need to be able to manage the fallout when fraud does occur. Because, no matter how good your fraud prevention tools are, breaches will happen. When they do, be prepared. Trying to track disputed transactions manually is a recipe for disaster—you’ll overwhelm your back-office staff and open yourself to lapses in Reg E compliance. You also don’t want to bungle your response to fraud in the eyes of your account holders; using visibly dated processes doesn’t inspire confidence or help retention. The bottom line is that manual, paper-based processes are no way to respond to sophisticated cyber fraud.

3. **Assess risk proactively**

Real-time monitoring and quick responses are crucial, but as transaction volume and speed increases, it becomes increasingly important to uncover risk before it has a chance to turn into loss. Timely, routine risk assessments are a must. Of course, risk reviews of originators are regulatory par for the course, but they’re also laborious and time consuming. This presents another opportunity for automation. Your FI has a lot of payments channels producing a lot of data; find a tool that brings together all of that information to produce a comprehensive, holistic view of the risk that your commercial customers pose. This should include data on everything from ACH transactions to outstanding loans, balances, deposits, wires—everything. Understanding the transactional trends and potential risk posed by your clients helps you limit exposure and avoid losses based on their behavior.

4. **Train users to spot fraud**

Users are often the weakest link in your security. Fraudsters know this and continue to target them in increasing numbers. Phishing attacks alone grew by 250 percent in the last year, according to Microsoft—and a single campaign in Q1 of 2018 sent out more than half a billion phishing emails! This means it’s crucial to train users—both customers and staff—on the best practices for avoiding scams. This includes tips for navigating social media, mobile channels, and apps (well over half of online fraud occurs via mobile platforms and over three-fourths of mobile fraud employs apps, rather than web browsers). FIs and other businesses hoping to teach their employees how to avoid phishing attacks can employ services and tools that simulate these attacks to test their users.

5. **Employ Multiple Layers of Security**

Managing risk takes a multilayered approach to security. To quote the IT guidelines of the Federal Financial Institutions Examination Council (FFIEC):

> Security threats can affect a financial institution through numerous vulnerabilities. No single control or security device can adequately protect a system connected to a public network. Effective information security comes only from establishing layers of various control, monitoring, and testing methods.

Your FI has multiple transactional channels, each with multiple exposure points—and your stored data is at risk of cyberattack as well. To reduce risk and prevent loss, it’s crucial to incorporate security and compliance tools and procedures throughout every channel. You should include measures like multifactor authentication, positive pay, behavioral analytics, endpoint interrogation, and more.
Balance risk management with user experience

While you can’t afford to make security and risk management a lesser priority, consumers sometimes do. Over 70 percent of financial consumers report being satisfied with easy-to-use authentication methods, while less than half cite a preference for methods that prioritize security over convenience.11

This makes it important that your security and risk management processes don’t introduce too much friction into user experiences. Numerous (or clumsy) sign-ons or unnecessarily flagged transactions can frustrate users—including both your customers and your back-office staff. Incorporating your security tools into an integrated platform with a single sign-on (SSO) can help with the former. Machine learning technology can help your analytics tools refine their interpretation of account holder behaviors to reduce false positives, while still detecting suspicious activity.

Remember, a big part of why transaction speed has become so important, at least to consumers, is because it’s convenient. Risk management is essential, but finding ways to integrate it seamlessly and efficiently into your user experiences is important too.

Conclusion: Keeping Up

When it comes to digital transactions and interactions, FIs aren’t just competing with each other, they’re competing with all the best digital experiences out there—including ecommerce giants like Amazon and Apple. Employing technology that’s sleek enough and fast enough is the only way to compete for account holders (especially with some of those big players introducing their own payments solutions).

In short, FIs have to keep up. It’s not enough to simply have fast payments options; you need a comprehensive payments strategy. This strategy has to contain payment options—including access to faster rails and new solutions—but it also has to contain ways to manage fraud, mitigate risk, secure your assets, and protect your users. Your payments strategy should also integrate into your FI’s larger technology and security strategy. It’s increasingly important to stay ahead of the technology curve as more and faster ways to transact business, make payments, and deliver experiences continue to emerge.

About Q2

Q2, a financial experience company headquartered in Austin, Texas, builds stronger communities by strengthening the financial institutions that serve them. We empower banks, credit unions, and other financial services providers to be an ever-present companion on their account holders’ financial journeys—helping them unlock new opportunities, increase efficiency, and grow their businesses. Learn more at www.q2ebanking.com.
Sources

2. www.consumerreports.org/digital-payments/mobile-p2p-payment-services-review/
Biographies

Debbie Smart, CTP, NCP
Senior Product Marketer, Q2

With more than 40 years of banking and cash management experience, Debbie’s role as senior product marketer is to understand Q2’s customers and prospects, leveraging market research and competitive intelligence to forge new partnerships and influence the capabilities of Q2’s product suite. Debbie has served on multiple boards, councils, and task forces, including the Association for Financial Technology Board of Directors; NACHA’s Payments Innovation Alliance; and the U.S. Faster Payments Council.

Brian Koenig, AAP
Product Manager, Q2/Centrix Solutions

Brian Koenig has been involved in the banking and financial services industry nearly 20 years, with experience in online banking, treasury management, fraud detection, and payments. In his current role at Q2, he serves as a product owner focusing on payment processing, reporting, and risk management solutions.