



# Business Payments Take Center Stage in Las Vegas

---

An **exclusive** compendium of thought leadership for the 2023 NACHA Smarter Faster Payments conference

## Financial Institutions and Their Clients Prepare to Ride the Faster Payments Rails

It's easy to take the "Smarter Faster Payments" tagline for granted here at the 2023 NACHA conference. After all, speed is the operative dynamic in the business payments world as we know it. NACHA's Same Day ACH, FedNow's Faster Payments platform and The Clearing House's RTP® are all driving business payments toward their real-time destination. With good reason, mainly because financial institutions stand to gain from the move toward faster payments, as do their business customers. Although the US has lagged behind other geographies in using real-time payment and settlement rails, for financial institutions the potential advantages include welcome changes to liquidity models and more visibility to cash management. For their commercial clients faster payments have similar advantages but we're also seeing serious momentum behind using them for B2B payments. **The organizations mentioned above all deserve kudos for raising the transaction limit in the US from \$100k to \$1 million.**

Smarter faster business payments come from tool kits that include fraud prevention and optimized user experiences and payment options that range from real-time to ACH. Banks banks and businesses need this wide range of on-ramps and rails that work best for their needs.

A quick look at some of the content tracks promise that these issues will be explored with depth and breadth. Among them are deep dives into fund transfer security procedures, detecting and deterring fraud schemes and maximizing embedded payment capabilities.



**But make no mistake, the star of the show will be faster payments.**

With that in mind we've assembled this compendium of thought leadership to complement the learnings attendees will from the event. You will get the experienced and expert perspective from Jessica Cheney here, Bottomline's vice president of product management and strategic solutions as she unpacks the advantages of real-time payments. You will also get a look at an exclusive global view of the real-time future as well as other hot button issues here including insider risk management at financial institutions. Finally you'll see links to The Payments Podcast and more research about B2B payments.

It's an exciting time for the payments industry. We hope the package we assembled here will provide evidence of that and give you a reason to learn more.





# Digital Banking Outlook: **High-Speed Rails Define Direction of Travel**

By: Jessica Cheney

This year, more than most, has many of potentially impactful factors when it comes to digital banking, and one sure shot. We don't yet know for example, how the general economy will behave as consumers contend with the continued rise of inflation and potential recession. We don't know how willing consumers are going to be

to share data and embrace the open banking principles that have gained traction in the UK and EU, but have stalled in the US. But one thing we do know is that at the end of the day – or the year for that matter – 2023 will be about the speed and accuracy of business payments.

The driver behind this is real-time/instant/faster payments (depending on the geography you're working in and the rails you're sending a payment through). In the US real-time payments have been being spearheaded by The Clearing House (TCH). To say it will see some new competition in 2023

**2023 will be about the speed and accuracy of business payments.**

is an understatement. The Federal Reserve will enter the market with its Instant Payments platform sometime in the late spring or early summer.

Federal government entrance will do more than shake up the market and push high-speed rails to the top of the “to do” list for finance leaders. It will expand access to high-speed payment rails beyond

the top tier financial institutions that currently use them. For some perspective, many sources, including a recent **PYMNTS** report, puts real-time transactions through current rails (TCH, NACHA) at **1.8 billion in 2022 with a spike to 8.9 billion by 2026.**

That's a dramatic growth curve for any business and proof that digital transformation isn't just a buzz phrase. Real-time payments is what digital transformation looks like.

It's important to point out that features like real-time payments are poised for growth in the commercial banking sector as well as retail.

Commercial banking needs to catch up to retail banking when it comes to payment mechanisms. Some of those mechanisms – particularly peer-to-peer payments – were accelerated by the pandemic when consumers were demanding low-touch payments. These B2C features will start to have a bigger impact next year.

For example,

## 45%

of bankers say they will **increase investment in mobile technology** to support B2B payments next year, according to research from the **Association for Financial Professionals.**

It's also interesting to note that the report stated:

**"Speed is critical for B2B payments. A majority of all survey respondents (54%) report that speed is the primary driver when choosing a payment method. And 62% of all survey respondents report that B2B transactions will benefit the most from faster/real-time payments."**

There's nothing but upside to real-time payments. Its momentum is the logical evolution of a trend started during the pandemic when consumers turned to peer-to-peer payments and contactless technology and businesses turned to accepting new forms of payment. It follows that real-time payments became a way not only for businesses to pay each other, but their employees as well. It has the advantage of allowing a company to hold onto their cash longer and only make payments at the required minute to take advantage of advantageous payment terms. Payments of any kind are first and foremost a liquidity tool that should be understood and utilized

in that manner. But with all this upside comes **one major concern for me and that's complacency.**

The attitude of "wait until next quarter" won't work during 2023, regardless of the economic picture. I think banks need to actively innovate new use cases and add on services around instant payments. There's really no benefit at this point of waiting for the Fed to make any more announcements about the FedNow service. We know what the message sets are (featuring the data-rich ISO 20022); we know what the production or live dates are going to be; we know the pricing structure and we know the technology partners. Delay will run the risk of customers seeing their bank as lagging in essential technology, which opens the door more aggressive competitors.

The need for speed is not limited to the US or the Fed. In fact, the urgency to adopt them in the European Union might be more dramatic. The EU finance commission closed 2022 by proposing an update to its 2012 instant payments regulations. It has four main aspects. The **first** would make instant payments universally available in euros. **Second**, it would make these payments more affordable, mandating that they

stay in line with pricing models for non-instant transfers. **Third**, it would implement an obligation similar to the UK's confirmation of payee which requires payment service providers to match the international bank account number on the name of the beneficiary. And **fourth**, it requires payment service providers to verify their clients against the EU sanctions list.

But there's will be a lot more going on this year in the EU, as my colleague Frederic Viard, head of products for Bottomline's financial messaging told me recently. He believes the shaky economy and continued geopolitical instability in the region will lead banks to exercise caution in their investments and prioritize business continuity. That translates to a focus on profits and the customer experience.

**"Protecting the customer as an asset will be achieved by continuing to invest in digital banking for an improved experience," Viard says. "These could drive to a broader adoption of new methods of opening new accounts and allowing more data access via open banking. All this must happen while ensuring compliance with regulatory mandates and managing liquidity."**

#### THE BOTTOMLINE:

Banks all over the globe must make 2023 the year of real-time and instant payments but they can't stop there. They need to actively look for innovative new use cases and add on services. For example, instant payments have added communication vehicles – many part of the ISO 20022 protocol – that can extend payment confirmation and avoid fraud. Banks shouldn't wait for someone else to figure out how to serve, protect and stay in touch with their customers. If they do, they may not be in very good shape come 2024.

# EXCLUSIVE RESEARCH: COMPETITIVE BANKING REPORT CLARIFIES REAL-TIME FUTURE

By: Vitus Rotzer

**No matter how you look at it, 2023 is shaping up to be a watershed year in the business payments and banking business.**

There's the recession that hasn't quite arrived and the spikes in goods and services that have showed up in a big way. There are real-time payments, ISO 20022, and the digital transformation needed to adopt them. And there are the continuing issues that need to be tracked closely around cross-border payments and security regulations.

In this landscape, we've been in the field since mid-year with a global banking survey that scopes "The Future of Competitive Advantage in Banking & Payments 2022." All the previously mentioned issues are covered in the survey, selected for their relevance to the future competitive set necessary to attract and retain customers. **The biggest departure from last year can be found in real-time payments,**



**which has risen from 40% in 2021 to 55% in 2022 as the top priority for banks and FIs over the next 12 months.** Next, mitigating fraud risk from 38% in 2021 to 53% in 2022.

If we had to pick the top finding from the report, we could stop there. But the report is stacked with important findings that will inform the ability to compete in 2023. **Among them:**

## DIGITAL TRANSFORMATION CONFIDENCE:

**Here we find a split between the confident (62%) and the sceptical (20%), with 8% not sure.** One will compete; the other categories should be concerned. The confident category needs to advance their competitive capabilities by staying abreast of new payments architecture and security regulations. The skeptical or not sure cohorts are most likely dealing from a standpoint of legacy architecture and will need to accelerate their digital capabilities quickly.

## APPETITE FOR CLOUD MIGRATION:

Here we find **60% are strong or extremely strong** in terms of prioritizing cloud migration 2022 Vs. **75% in 2023.** Analyzing this number leads to two possible conclusions: either SaaS-based technology is approaching critical mass and banks have already migrated or, they're more doubtful of its effectiveness compared to last year. We're going with the first analysis.



## As Bottomline's head of SaaS solutions Charles de Rougé told us:

"Using a hosted, standard, secure, SaaS-based platform to connect, control, compete and comply inspires confidence that your capabilities evolve according to market expectations and the demands of your internal strategy regarding appropriate investment, product development, and the generation of new revenue streams. Secondly, you reap the rewards of a constantly evolving platform optimized by best practices and driven by the collaboration and innovation of vendors and market players."



### OBSTACLES TO IMPROVING PAYMENTS INFRASTRUCTURE:

As it was last year, legacy systems were the top concern at 27% of respondents. We also saw that 13% of respondents have a lack of IT resources to build more efficient infrastructure. **This is proof positive that it's often too expensive for most institutions to maintain heavy infrastructures on-site.** These disadvantages impact the ability to scale on-demand and future-proof systems. The solution: partner with the right supplier to leverage their expertise and bandwidth – whether that is via SaaS, Service Bureau, or a trusted Fintech partner. These options keep your development to a minimum by utilising the right partner who is already audited and compliant.

### EMBRACING THE REAL-TIME REVOLUTION:

As stated earlier, **by displacing digital transformation at 63% this is the most important finding in this year's survey.** That's a positive development but the second place priority - payment fraud detection and prevention with 54% - is an unfortunate negative factor that will exist as long as digital banking does. Improved regulation and best practice solutions such as Confirmation of Payee and Bank Account Verification will help. So will leveraging the benefits of the ISO 20022 messaging standard.

### IMPORTANCE OF REGTECH:

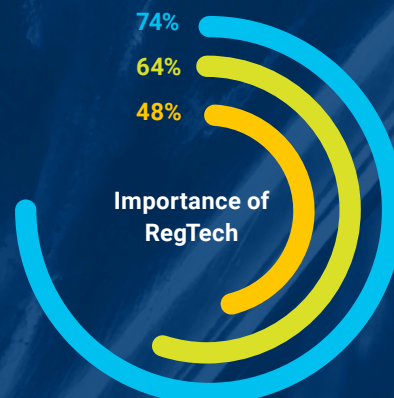
Last year **64%** said regulations would be more important than in 2020. That jumped to **74%** this year with **48%** characterizing "remaining complaint" as very challenging. Regardless of how tough it is banks need to see regulation as a positive market dynamic. As Becky Clements, Head of Industry Engagement, Pay.UK told us:

**"You can't have harmonization without standardization".**

So, regulation and compliance will continue to drive change. The tools are out there and so banks and FIs need to be better collaborators."

### THE UPSIDE OF ISO 20022:

Here's the predictable response: 53% said better data and data analytics would be the most important feature of ISO as it relates to cash management. But here's the surprise: **56% said improving fraud monitoring and management tops the chart.** Our analysis is that the advantages and use cases of ISO 20022 have not been settled and it's an issue we look forward to tracking. Data and fraud prevention go hand-in-hand. If the data from ISO can be incorporated properly, operations and treasury will find risk scoring to be more efficient. It's also less work for the compliance department as better data should lead to more accurate sanction screening.



### CROSS-BORDER OUTLOOK IS CLOUDY:

In 2021 24% rated lack of visibility on payments status as the biggest cross-border pain point. That jumped to 35% this year when it actually should have decreased due to initiatives such as SWIFT gpi and ISO 20022 standardisation. This potentially points back to slow adoption levels or delays in ISO readiness. **It begs the question:**

**What is it that banks want to see in cross-border payments status?**

It's an important question as the increase in revenue from cross-border should follow new fee-based pricing structures and multi-lateral platforms that enable global payments through a single connection. We also think banks want to see an enhanced customer experience with more security and efficiency through tokenization, governance, and rich data.

**Make sure your financial institution is on track to maximize on the changes impacting the payments ecosystem and accelerate your digital payments transformation strategy today – that is where true competitive advantage can be leveraged. Also, make sure you have your voice heard and start the live comparison survey now.**

[READ REPORT](#)

# INSIDER FRAUD Q&A: NATIONAL THREAT CENTER EXPERT DISCUSSES UNIQUE ASPECTS OF BANKING

By: Nick Griffin



Insider fraud is one of the emerging threats for banks and one of the emerging experts in this space is

**Sarah Miller.**

Her work as an insider threat researcher for the CERT Division of the Software Engineering Institute, based at Carnegie Mellon University, includes the December 2021 report "Spotlight on Insider Fraud in the Financial Services Industry". The report collected over 1,600 analyzed insider threat incidents. **The result was a detailed body of evidence showing that 25% of all reported insider threat cases come from the financial service industry.** We connected with her for a special IFAW Q&A.

**Q:** We've done a lot of research as a company and a lot of case work, but your report on insider fraud and banks was among the most impressive work that we've seen. So how did this all come about? How did you pick insider fraud? And how did you pick banks?

**Miller:** When I was working at Carnegie Mellon University, I was the steward of the National Insider Threat Center (NITC), insider threat incident corpus, which is a long way of saying that the NITC **collects data on insider threat incidents at the US federal level for analysis** and eventually to produce reports like the one I was involved in. At the center, I was responsible for making sure that we added good information and that we were analyzing it actively. My work

also built on the excellent foundation of research from Randy Trzeciak, Dawn Capelli and Andy Moore. It's important to mention them here because they built the NITC.

**Q:** What did you find that was unique about banks and insider fraud?


**Miller:** A couple of things. One of those is the intermingling of the incidents. We see cases of stolen identity refund fraud schemes, which can involve a number of types of individuals and organizations. In some cases multiple banks were involved and included a group of between **10 and 30 different people, all working to steal information and money from banks.** Then they essentially launder it through check cashing facilities and other methods.



You can see just how interconnected these banks are and that these employees have connections to one another, even if they're working in different organizations.

**Q:** Was there a persona that surprised you about the insider fraud profiles?

**Miller:** First, let me say that there is no one profile. That's one of the things that's unique here. It fascinated me that we saw employees that aren't just tenured but also in some sort of management position. And obviously with those positions of authority comes certain privileges and a level of trust.

 There was a case I read about recently, just in my own research, where somebody at a credit union **intentionally implemented a faulty bank secrecy program so that they could engage in money laundering.**

And I've seen other cases where an executive **intentionally misled their direct reports to manipulate a situation or further a scheme.** That's not something commonly seen in other sectors.

**Q:** Let's say I'm the CEO or even the Chief Human Resources Officer at a financial services company. We don't want to create a culture of fear. But we do want to create a culture of safety. How does that get communicated? Have you seen anybody do it well? Have you seen anybody do it poorly?

**Miller:** Have I seen anyone do it poorly? That's a little easier to answer. I've heard of cases where people name and shame departing employees that maybe didn't follow all of the policies, rules and regulations. That can be very scary to a workforce. But you can't go wrong when insider security is part of the conversation that you have with employees. It's not just something that happens during National Insider Threat Awareness Month, or National Cybersecurity Month. I've seen organizations do it well by rewarding employees with actual awards and certificates, and by celebrating people that do a good job of completing their training, identifying phishing emails or participating in security awareness events.

**Q:** So the collusion number in your report absolutely blew us away (31% of all insider fraud is due to collusion among one or more employees). Did it surprise you? And did you have a sense as to whether or not it's collusion internally or with an outside actor?

**Miller:** I've been interested in that because at one level insider fraud because fraud can be such a simple process of "I take the money out of the tail and go about my day." But if you don't want to be caught, it requires a lot of healthy resources that an employee might not have access to. And I would say again, something else that makes finance so interesting is that it's not just working with peers, it's working with those outside actors, including other financial institutions. What's scary is that it's not just other insiders,

especially with those stolen identity refund fraud schemes which can be hard to detect. Organizations might not find out about it until law enforcement comes knocking.

**Q:** The report ends with 21 best practices for fighting insider fraud. Are there a couple of things from that paper that you think are particularly relevant now?

**Miller:** The new one that I advocated for is **learning from past insider incidents.** And I would say the sort of overarching kind of message of that paper and some of the best practices is that **you don't have to reinvent the wheel.** There are others in the community of insiders, fraud practitioners and investigators that want to help each other that you can connect with that have learned from past incidents and want to share and collaborate. I would encourage people to seek those colleagues out. Insider threat detection is a relatively small community within security, which is already a small community. There are other people in organizations that you have already done business with that have already done the hard work of identifying what your critical assets are.

**You don't have to start from scratch.** There are people within and outside of your organization that want to help you do a better job of preventing insider fraud.



# DOES THE NEED FOR SPEED INVITE PAYMENTS FRAUD VULNERABILITY?

By: Ruud Grotens

As **real-time payments** continue their international climb toward critical mass, you have to wonder how one of its central issues has become so confused. While the payments industry from Washington DC to London to Mumbai should be discussing the cash flow and real-time settlement advantages of this newest payments technology, instead, we're focused on fraud. That's a legitimate concern, but **are real-time payments really more vulnerable to fraud?**

Here's an example of the issue in, real time. I was on a panel recently for a webinar hosted by the Association of Certified Financial Crime Specialists (ACFCS). The moderator asked a poll question: What do you think is behind the rise in real-time payments fraud? The answer was the speed and scale of the payment mechanism, but it strikes me in hindsight that the question should have been: Have you noticed more fraud activity around real-time payments? In a recent

report commissioned by Bottomline with Themis, 51% identified the increasing speed and volume of online payments as the greatest contributor to fraud risk. But a recent study by **PYMNTS.com** shows that about 10% of respondents listed lack of fraud risk as the most important feature of real-time payments. So

**Fraud rates will rise for real-time payments as more countries adopt them, will be used for higher ticket payments, and will likely attract more bad actors.**

we have been forced to assume (as is safe and responsible) that fraud surrounds the irrevocability of real-time payments.

Before I go forward, some semantics. I will use real-time payments interchangeably in this piece to represent the world of its labels, from instant payments (EU and US Federal Reserve) to faster payments (UK).

## LEARNING FROM BANKING HISTORY

As I said, this is a worthwhile debate and better to err on the side of caution. Let's assume that fraudsters are hard at work trying to find ways to take advantage of real-time payments. And here, it's worth looking at the history of instant payments.

When instant payments were first introduced in the UK in 2008, banks managed to reduce fraud losses

by implementing real-time detection solutions that blocked any suspicious transactions, but only after suffering some steep losses. We will get to the importance of ISO 20022 in the next section, and the next level fraud prevention it provides, but those early fraud detection efforts helped instant payments to gain awareness despite their weaknesses.

So, what are the lessons learned? Firstly, early preparation is required as fraud rates are highest when new real-time payment schemes are rolled roll out. Fraud rates will rise for real-time payments as more countries adopt them, will be used for higher ticket payments, and will likely attract more bad actors. Real-time payment fraud solutions need to be enhanced and stress-tested, able to

**51%**

identified the **increasing speed and volume of online payments** as the greatest contributor to fraud risk.

**10%**

listed **lack of fraud risk** as the most important feature of real-time payments.

block transactions in real time from day one. Banks and other businesses will require more capacity to handle real-time volume and manage real-time fraud. So as an industry, we need to prepare ourselves and be ready for what is coming.

ISO 20022 was introduced in 2004 but has found its true calling with real-time payments. It will be key in driving real-time payment schemes for cross-border settlements in the coming years. One of its aims is to ensure interoperability between financial institutions and separate countries. Its ability to carry rich data sets will help move through fraud protection. And it will also help to better structure that data and improve overall quality compared to legacy messaging standards.

For example, ISO 20022 contains around **ten times more data** about each payment, shared with participating banks and beneficiaries through the transaction's journey to its final destination.

This data includes information about the purpose of the payment and its original source. For example, in the Netherlands, ISO fields share the fraud scores from the sending party to the receiving party. This

enables the receiving party to better judge borderline cases where the information may be insufficient to flag a transaction.

### RISK MITIGATION IN REAL-TIME

When it comes to **real-time fraud**, risks appear within milliseconds. Where unusual or suspicious customer behaviour is detected, it is good practice to challenge the customer with authentication, i.e., extra steps to prove that the customer is the 'real customer'. Only if the authentication is successful will the payment proceed. Otherwise, it will be blocked. So instant payment networks have rules outlining the timeframes for conducting transactions (often within 10 seconds) but offer exceptions when suspicious or fraudulent activity is detected. You can imagine that when the added element of secure customer authentication was discussed during the introduction of the EU's Open Banking legislation, PSD2, stakeholders felt there was too much focus on anti-fraud measures and not enough attention on the customer experience. So businesses were concerned that secure customer authentication would cost them a large percentage of their online business. It didn't, and therein lies a lesson for those who believe anti-fraud measures will slow real-time payments.

### THE BOTTOMLINE:

Back to the data points. The PYMNTS.com study mentioned earlier found that **75% of US financial institutions using real-time payments report lower rates of fraud than those who don't offer it**. Granted, real-time accounts for about 1% of all transactions in the US. Know this: Fraud happens, bad actors flock toward new technologies, and responsible financial leaders should act proactively. Seeing fraud as an obstacle to adopting faster, instant, or real-time payments, depending on your geography, is a short-sighted approach. The primary functionality to consider for a payment fraud solution is risk-based detection that will minimize the impact on non-risky client behavior and maximize impact on high-risk behavior.



**Fraud happens, bad actors flock toward new technologies, and responsible financial leaders should act proactively.**



# RESOURCES



## **PAYMENTS PODCAST: REAL-TIME PAYMENTS HAVE ARRIVED ... WHAT ARE WE WAITING FOR?**

Bottomline's Jessica Cheney discusses balancing caution with tremendous opportunity in the context of real-time payment adoption in the US, sharing her views on how banks that are too cautious and slow to pull the trigger face becoming laggards and losing their competitive advantage.

▷ **LISTEN NOW**



## **PAYMENTS PODCAST: PAYMENTS MODERNIZATION: IS FRAUD PREVENTION PLAYING CATCH UP?**

Fraud experts Ruud Grotens and Eric Choltus scope the intersection between payments modernization and payment fraud prevention. In this discussion, we dive into whether fraud measures are managing to keep pace with the latest in payments innovations such as ISO20022, cross-border payments, and real-time payments.

▷ **LISTEN NOW**



## **INFOGRAPHIC: FEDNOW: FASTER PAYMENTS RAILS GET FEDERAL COMPETITION**

It is arguably the front runner for the biggest story in payments for 2023. When the FedNow faster payments platform launches sometime in the late spring or early summer of next year it will create a new real-time payment infrastructure that exceeds the reach of private sector providers The Clearing House and NACHA. Concerns about interoperability with those systems still abound. But at its core, there's no doubt that FedNow will expand the scope of faster payments to more banks, more businesses and more consumers. Bottomline has assembled the infographic [linked here](#) to serve as a resource for banks and other businesses as the chatter around FedNow grows toward its eventual launch.

**LEARN MORE**



#### CASE STUDY:

#### EASTWEST BANK STEPS UP TO SUCCESSFULLY RECEIVE AND SEND DATA-RICH ISO 20022 MESSAGES

EastWest Bank had the challenge of complying with the new ISO 20022 message format while managing the impact on their core banking system (T24) and the availability of IT support. Rodel Garcia, Head of the Fund Transfer Department at EastWest Bank, explained, "The migration project coincided with major enhancement projects on T24, and so the strategy was to keep the IT support requirement on T24 at a minimum, but still be able to comply with the BSP's requirements and continue to participate when the new PhilPaSS Plus went live."

[LEARN MORE](#)


#### RESEARCH REPORT:

#### CFOs FIND A RECIPE FOR SUCCESS

We quantified how well-connected CFO offices of today are to the data, talent, and tools necessary to get the job done, as well as further understand what areas of connection are priorities for improvements in the near future. This report is a deeper look at the results of a June 2022 survey of high-level finance leaders, dominated in this case by CFOs and vice presidents of finance

[LEARN MORE](#)


#### RESEARCH REPORT:

#### 2022 B2B PAYMENTS SURVEY REPORT

The 6th annual B2B Payments Survey was taken by over 800 payment professionals across the globe, and sought to determine the viewpoints of both bank and corporate respondents across multiple areas of payment development. The results include insights on top challenges; use of AI and RPA; areas of focus for efficiency improvements; use and view of APIs; payment fraud experiences; innovation plans; and even the level of B2C offerings by banks.

[LEARN MORE](#)