The

2022 Digital Payments Guide For Corporate Payments

PYMNTS.com | LexisNexis® RISK SOLUTIONS

February 2022

The 2022 Digital Payments Guide For Corporate Payments, a PYMNTS and LexisNexis® Risk Solutions collaboration, examines the challenges organizations face in managing financial data while meeting changing global payments requirements. It also illustrates how best practices in payments processes can help organizations sustain long-term growth.

The
2022 Digital Payments Guide For Corporate Payments

PYMNTS.com | LexisNexis® RISK SOLUTIONS

The 2022 Digital Payments Guide For Corporate Payments was done in collaboration with LexisNexis® Risk Solutions, and PYMNTS is grateful for the company's support and insight. **PYMNTS.com** retains full editorial control over the following findings, methodology and data analysis.

TABLE OF CONTENTS

Introduction

Strategic enterprise resource planning (ERP) is the foundation of any organization's long-term success. A savvy ERP strategy leverages big data to inform everything from workflow management to technology adoption and risk management policy, allowing organizations to optimize core business operations and support long-range fiscal goals. The success of any ERP initiative, however, is wholly dependent upon key drivers of business growth — such as digital payments processes — operating seamlessly.

If an organization uses a robust digital ERP platform, it likely will have access to extensive data on the efficacy of its payments processes and how they impact the company's bottom line and long-term risk management strategy. Even if an entity does not have the benefit of real-time insights on digital payments efficiency, it likely is well aware that its ability to scale and manage risk over time hinges upon its ability to execute the basics — such as managing data and corporate payments — from day one.

Additionally, managing digital payments and their corresponding data effectively is important for another reason — regulatory compliance, including cross-border transaction reporting to compulsory know your business (KYB), know your customer (KYC) and anti-money laundering (AML) monitoring. Digital payments processing can be at risk if your data management system is outdated or unable to scale efficiently.

Since regulatory compliance and business operations efficiency are no less important than the development of new revenue streams to any business's success, removing unnecessary friction from digital payments likely is a priority for most organizations.

The 2022 Digital Payments Guide for Corporate Payments, a PYMNTS and LexisNexis® Risk Solutions collaboration, examines the challenges organizations face in managing financial data while meeting changing global payments requirements. It also illustrates how best practices in payments processes can help organizations sustain long-term growth.

Managing bank master data — keeping on top of changing global payment requirements

Amidst the vast data quantities organizations generate and process every year, bank master data is among the most difficult to manage manually and among the most critical to business operations. Effective bank master data management requires a robust ERP platform with seamless integrations with payment services or, if monitored manually, constant vigilance and access to extensive and recent global banking data.

Here are three reasons why managing bank master data presents a challenge to many financial institutions (FIs) and corporates alike:

KEY PAYMENTS DATA OFTEN CHANGES.

Data is crucial to risk management: KYB, KYC and AML mandates require accurate record keeping at every stage of a transaction for compliance. Yet key components of banking data — such as customer data, bank keys, control data and even bank country codes — can change with little warning, causing payment delays, misdirected payments or payment failure. A bank merger, an address change of a bank's headquarters or a change in payment service provider can instantly impact the user experience for consumer and business banking clients.

SANCTIONED BANKS MAY STILL INITIATE AND RECEIVE TRANSACTIONS.

Vendors and suppliers that do business with companies around the world may bank virtually from anywhere. This means that even after FIs or businesses have complied with KYB, KYC and AML regulations, there is the matter of keeping track of current sanctions or restrictions that may or may not be related to these three concerns. Making payments to or through accounts held at banks sanctioned by regulatory bodies such as the U.K. Financial Conduct Authority, European Union, The U.S. Office of Foreign Assets Control or the United Nations can result in a corresponding bank or corporate entity garnering a fine for regulatory noncompliance. Access to an extensive list of sanctioned banks is essential for long-term risk management.

FINANCIAL TECHNOLOGIES ADD COMPLEXITY TO COMPLIANCE.

The rise of advanced financial technologies has made regulatory compliance more complex for both FIs and corporates. New transactional data architectures and device-based "pass-through" payments involved mobile app companies, FIs and corporates with newer interactions that redefined how payments, financial data and FIs are classified and regulated. Despite the challenge of maintaining compliance when processing newer types of transactions, such as virtual currency mobile payments converted into cash and deposited into traditional bank accounts, global banking regulatory bodies are developing new mandates that will require FIs and corporates to overcome data management obstacles to remain in compliance.

Here are three of the most common bank master data issues and how to solve them:

BANKING DETAILS "FRESHNESS"

Adopting an ERP platform solution that integrates daily updates to global banking data via ASCII and XML feeds into payments processes is a simple way for organizations to ensure payment details are more accurate and that watchlists for sanctioned banks and other risks are well maintained. Global payments data also can be updated on a daily basis manually.

DUPLICATE BANK MASTER DATA

Duplicate data may have the same impact as inaccurate bank details, causing delays in transaction processing or triggering false security flags. Using an ERP system that allows banking data to be built and maintained dynamically allows for easy edits of erroneous or duplicate data. Manually maintaining bank master data requires scrupulous attention to data-entry hygiene and regularly monitoring new banking details for changes.

TRANSACTION LATENCY

Following a review, bank data sometimes can change and payment delays may occur. Working with a technology solutions partner that facilitates last-minute domestic and international payment routing may solve this problem by providing enriched banking data — which includes the information required to route payments efficiently, more accurately and in compliance — to the ERP and payments processing platforms. Enriched banking data also can be used to manually validate bank data.

While managing bank master data is an essential component of a successful ERP policy, the efficient management of vendor master data also is a critical element of long-term risk mitigation.

Duplicate data

may have the same impact as inaccurate bank details, causing delays in transaction processing or triggering false security flags.

Vendor master data — capturing more accurate payment instructions from suppliers and partners to ensure straight-through processing (STP)

Vendor master data, like bank master data, is a powerful resource that can optimize or degrade the outcomes of core business processes. For corporates, delays due to out-of-date payments instructions can create a cycle of poor user experiences, including halting crucial payments that keep supply chains on pace and creating slow or cancelled orders due to vendor payment failures.

For FIs, inaccurate payments data can cause damaging delays, interrupt third-party data validation processes in consumer-facing products and limit critical payments transfers to business-to-business (B2B) clients network-wide. One key to higher rates of STP is access to an ERP-connected treasury management system (TMS) that offers reliable vendor data that might range from payment instructions to near real-time user authentication that is automatically (or easily manually) updated in your vendor master data table.

Best practices for vendor onboarding platforms

Another important promoter of high STP rates is a data-driven vendor onboarding process that seamlessly integrates with an existing ERP and/or TMS solution. Here's why:

VENDOR RISK ASSESSMENT IS CRITICAL FOR REGULATORY COMPLIANCE.

FIs and corporates need easy access to extensive data on every vendor. When that data is accessible through an organization's ERP platform — its fulcrum of decision-making — it is easier to assign Bank Secrecy Act/AML risk ratings to potential vendors and facilitate better choices.

VETTING VENDORS IS AN ONGOING PROCESS.

Vendors' business practices may change over time, but an organization's regulatory and customer service obligations will remain static. Consistently monitoring vendor business practices and regulatory compliance is a must.

KYB STANDARDS MAY VARY FROM REGION TO REGION, BUT INTERNATIONAL REGULATIONS REQUIRE A GLOBAL OUTLOOK ON RISK.

Vendor onboarding practices should aim for the highest levels of due diligence — even if your vendor's country of origin (or an organization's) has a lower standard of identity verification than international regulatory bodies.

For FIs, inaccurate payments data can interrupt critical payments transfers to B2B clients network-wide.

What vendor payments data should be validated at point of capture?

Critical information includes:

- Payment instructions, including banking details
- Per-transaction bank and account holder data, including FinTech and “pass-through” entities
- Vendor’s authorized agents and principals’ identities, including identity authentication documents
- Vendor business registration information
- Near real-time credit risk scoring
- Watchlist scan results

Automatically enriching the vendor payment information before and after onboarding

Automatically enriching vendor payment information is not a linear process when completed manually, yet fresh data is crucial to ensuring an organization remains compliant through each vendor interaction. FIs and corporates must review fraud prevention, identity verification, compliance, politically exposed persons (PEP) and watchlist screening results in addition to basic credit risk assessments before deciding to onboard a supplier. An ERP platform that offers extensive vendor screening and onboarding features can automate many of the administrative tasks involved in enriching vendor payment information, allowing an organization to simply search for a vendor to find near real-time granular insights into their risk level and current payments instructions. In absence of an ERP platform, the above vetting tasks are typically carried out manually. Whether using an ERP platform or running manual searches, the following are a sample of key regulations and watchlists to grade potential vendors against:

- Bank Secrecy Act / USA PATRIOT Act
- AML regulations
- OFAC sanctions
- AMLD5
- Society for Worldwide Interbank Financial Telecommunication (SWIFT), Automated Clearing House (ACH) and Fedwire protocols

In addition, vendors should be screened for their relationships to the following:

- State-owned enterprises
- PEPs
- Adverse media
- Sanctions
- Entities associated with sanctions
- Regulatory enforcement actions
- Conflicting or contradictory registration data

Five best practices for using a vendor onboarding platform

Vendor relationships are too complex — and too laden with hidden risks — to enter into without exceptional data and powerful analytical tools at the ready. Here are five key enhanced due-diligence features to look for when selecting a vendor onboarding technology solution with your ERP platform:

Near real-time verification of vendor business status data, including automated watchlist screening

Instant authentication of vendor identity with automated forensic analysis of ID documents from vendor's country of origin

Near real-time verification of current banking data, payments instructions and risk indication at point of capture

Robust, ongoing vendor risk assessment monitoring and automated vendor risk scoring features

Automated global regulatory compliance screening inclusive of KYB, KYC and AML mandates for all vendors

The
2022 Digital Payments Guide
For Corporate Payments

Exceptional data and powerful analytical tools are key to a successful

vendor onboarding process.

Best practices for **creating payment files**

Accurate payment file creation is important to corporates for both compliance and revenue flow management. A single data entry error on a payment file can cause costly interruptions to payment flows and trigger compliance audits.

Accurate payment files are critical to regulatory compliance and payments processing efficiency.

Step One

Identify issues before submitting payment files to your banks

Automate payment file creation to avoid manual data entry errors

Automating payment file creation and dynamic updates through an ERP solution is recommended for speed and accuracy.

Use a robust ERP with access to real-time data

FIs and corporates using a powerful ERP platform — or those with access to exhaustive ERP near real-time data — easily can keep payments data up to date within their bank master table through automation (or detailed manual entry).

Be mindful of critical datasets

Digital payment files should include the following information for all clients and vendors:

- SWIFT/Bank Identifier Code (BIC)
- Bank branch codes
- Institution name
- Institution address
- Sanctions
- Office type
- Contact details

Step Two

Ensure ISO 20022 compatibility

This year, FIs will begin to migrate from SWIFT MT financial messaging to ISO 20022, a new global open standard for payments data transfer and messaging that will replace the legacy SWIFT MT model.[1] ISO 20022 provides rich, granular transaction data through XML feeds, making it simple to integrate with existing ERP platforms and payments services. Corporates and FIs currently unable to accommodate ISO 20022's use of their existing technology stacks would be wise to consider using a TMS or an advanced ERP solution that automates ISO 20022 technology integration.

Step Three

Check banks' and vendors' current compliance status

Checking banks, accounts and vendor relationships routinely is essential for compliant end-to-end payments processing. Ensure payment files are compliant at their creation and constantly updated with dynamic data to reflect any changes in vendor or bank status or relationships.

[1] Author unknown. ISO 20022. https://www.iso20022.org/ Accessed January 2022.

Adopting new digital payments channels for **business growth**

Modern digital payments adoption — including using contactless payments and integrating virtual currencies into eCommerce models — can offer corporates and FIs new efficiencies when paired with a robust ERP or TMS platform. Enterprise-grade digital payments solutions allow organizations to collect and process payments from connected devices and consumers or clients globally. Records are updated in near real time and revenue data is easy to review, compare with ERP benchmarks and transform into actionable insights for the entire organization.

Here are some ways in which digital payments adoption can serve as a key driver of business growth:

- Using an ERP or TMS solution with digital payments allows organizations to monitor payments data, including any newly updated payment instructions, while deploying powerful user validation and transaction management tools across the organization.
- Integrated digital payments and ERP platforms automatically can enrich payments data to limit errors and provide extensive, more accurate and more compliant reporting.
- Digital payments platforms that are compatible with automated compliance features on ERPs help reduce friction from cross-border payments processes, limiting user validation delays based on incompatible KYB, KYC or AML standards.

Emergent payments technologies can create new business value

Emergent payments technologies can create intuitive customer experiences for users and help boost consumer loyalty to brands, retailers and FIs. Popular digital payments methods include:

DIGITAL WALLETS

Digital wallets store credit, debit and prepaid cards and even digital currency virtually. Some use tokenization, which replaces card numbers with randomly generated digits. This, along with other dynamic data elements, can make digital wallets hard to spoof. Many digital wallets are contactless, allowing users to "tap" their mobile devices at an enabled point-of-sale (POS) terminal.

HYBRID ONLINE-MOBILE PAYMENTS

A hybrid online-mobile system allows consumers to use their phones with their computers to carry out tasks such as user authentication and payment validation.

CONTACTLESS PAYMENTS

Following a review, bank data sometimes can change and payment delays may occur. Working with a technology solutions provider that facilitates last-minute domestic payment routing may help solve this problem by providing enriched banking data — which includes the data required to route payments efficiently, more accurately and more in compliance — to the ERP and payments processing platforms. Enriched banking data also can be used to manually validate bank data.

While managing bank master data is an essential component of a successful ERP policy, the efficient management of vendor master data is an equally critical element of long-term risk mitigation.

In each case, digital payments technologies that integrate with an enterprise-grade TMS or ERP platform with near real-time data access empower the authentication of bank and account holder details, the isolation of errors and the initiation of corrections. They also would enable the addition of enriched payments data to ERP, TMS and payments processing platforms in near real time and would allow payments to be directed more efficiently through cross-border and domestic payments networks based on near real-time data.

Automating manual steps in the payments flow to **optimize resources and drive efficiency**

Whether creating a payment file or vetting a new vendor, saving time without sacrificing accuracy is key. Automation is a solution that can help organizations scale payments without friction.

Automation does much more than simplify payments processes — it helps remove administrative burdens from payments operations.

Best practices for building payment flow without manual steps:

AUDIT MANUAL DATA ENTRY PRACTICES.

Manual data entry can be prone to errors, and its use may increase risk when it comes to compliance reporting and payments instructions management. Implementing automation whenever possible via an ERP or TMS system helps mitigate these risks.

USE A PAYMENTS API TO SYNCHRONIZE PAYMENTS PROCESSES.

If your TMS or ERP platform offers it, a payments API solution can be integrated along your payments flow to validate, update or offer visibility over payments processes.

LEVERAGE DYNAMIC DATA.

Ensure automated payment file creation and editing is informed by near real-time data and distributed according to current contact details for all relevant entities.

Automation does much more than simplify payments processes — it helps remove administrative burdens from payments operations. Payments operations personnel then can be redistributed to add more business value and play a unique role in vendor onboarding and digital transformation support — ranging from serving as customer service liaisons to ensuring employee training in new technologies is efficient and impactful.

Best practices for utilizing digital **onboarding portals**

Automation is key to an effective digital onboarding process for customers or vendors. The efficacy of automation is dependent upon the quality of the data that informs the onboarding process, and inaccuracies can result in transaction processing delays and security risks. Here are four principles that should inform the digital onboarding process or selection of an ERP or TMS technology solutions partner:

A POWERFUL DIGITAL IDENTITY VALIDATION SYSTEM AND NEAR REAL-TIME DATA ACCESS

An ERP or TMS partner or digital onboarding portal should use the latest technology to validate user identities in near real time and automate recording of shifts in dynamic data.

PROCESS VISIBILITY

A digital onboarding platform or technology should be user-friendly, allowing the organization to view customer or vendor data across each channel or touchpoint in near real time.

ONGOING SMART AUTHENTICATION USING MACHINE LEARNING (ML) AND ADVANCED BEHAVIORAL ANALYTICS

Cybercriminals use advanced technology, and so should any organization. A digital onboarding process should use advanced tools to monitor user or client risk signals over time and assign new risk assessments as needed.

Transforming onboarding processes digitally can produce long-term benefits for organizations.

Three benefits of improving digital onboarding data capture:

FASTER USER AUTHENTICATION

An API-based digital onboarding solution automatically can add required banking details so customers can avoid manually entering their information during payment setup.

FEWER FAILED PAYMENTS

Automated payment instructions matching can limit failed payments by ensuring last-minute routing is more accurate.

EFFECTIVE RISK MITIGATION

Improved data capture allows organizations to provide payment files and vendor data based on more up-to-the-minute data that is more compliant and granular in detail.

Case Study

lsq

Decoding Digital Transformation

Digital transformation is a long-term goal for many corporates, but implementation can be intimidating. According to Dan Ambrico, CEO of working capital solutions provider LSQ, how a corporation launches its digital payments strategy is as important to outcomes as its timing of doing so. He said that the pandemic accelerated digital transformation among corporates, affecting how they see everything from accounts payable (AP) to accounts receivable (AR) to customer relationship management.

The problem, Ambrico said, is that implementing a digital payments solution can be resource-intensive for companies, especially with AP and AR flows adding to the complexity of launching a digital payments approach.

"It's very much about a resource shortage, particularly when you get into lower enterprise middle market," he said. "The AP teams are relatively small, they're spread thin and they're trying to keep their heads above water. Managing an implementation process or digitization process is just sometimes a bridge too far."

Additionally, digital payments processes and AP/AR solutions can be a jumbled mess due to the way the industry has evolved over time. Corporates may have to navigate a maze of payments products and accounting solutions that don't play well together. "A lot of these companies have consolidated, and there's a hodgepodge of systems. So, you're dealing with a business that has a bunch of different legacy systems that have all been kind of smashed together over the years, and it's very hard to untangle that," he said.

According to Ambrico, the first step for corporates is to look at the core of existing payments systems — such as AP and AR or how vendors or suppliers send and receive funds — and look for processes that are inefficient or simply too cumbersome to scale.

Vikas Shah, LSQ's chief revenue officer, added that organizations should avoid leaping into digital payments before they have untangled how their company operates as a whole with respect to sending and receiving funds.

"Don't just jump on digital payments for the sake of jumping into digital payments," he advised. "Think about process and automation for AP and AR first, before you embark on digital payments. What can happen is you may try to do an ad hoc project on digital payments, and then you realize your AP and AR processes are so broken that the value of digital payments is often not materialized."

Shah explained that a better idea is to see digital payments as part of an overall process improvement for the entire organization. Corporates should implement digital payments and related innovations such as embedded finance in a way that delivers value and added efficiency for every aspect of business operations.

"Our caution statement is really: understand your constituents and your user base, whether it's on the supplier side or the customer side or [the] partner side, and figure what value you would be adding to those constituents before jumping on a project," he said. "What companies and platform technology vendors need to start thinking about is 'what additional value am I adding as part of that process?'"

Answering that question, Shah believes, is key to making digital payments (or any digital innovation) part of a sustainable growth strategy for any businesss.

Executive Insight

Leslie Bailey, vice president of financial crime compliance and payments for LexisNexis® Risk Solutions, explains why good data hygiene and efficient data management are key components of long-term risk management.

Why is the effective handling of bank master data essential for FIs' risk management?

Vigilant global bank master data management is critical to mitigating risk to your FI and corporation, and it requires a seamless integration to a robust ERP platform. To achieve vigilance, an automated process around bank master data hygiene is imperative, since bank master data loses its freshness as soon as it is updated.

There are many challenges created by inaccurate global bank master data for FIs and corporates alike, and to name a few: manual processes allow for lags in maintenance and create room for errors, failed payments create operational internal inefficiencies of time and money — also creating a poor customer experience in the most competitive environment to date and creating financial compliance risk at other points in the compliance process.

One of the most common bank master data issues is data "freshness." To solve, use an automated process to update bank master data in near real time in the ERP platform, like an ERP data file or an API that easily integrates to verify and enrich data as it is captured and as the data is used at other points in the payment process.

Failed payments slow down or stop the speed of payments execution, cause operational inefficiencies to investigate and resolve, generate expensive remediation fees and result in an unhappy customer in today's environment where alternative providers are only a click away.

Finally, if the front-office-to-back-office data hygiene solution is not automated at both the point of capture (onboarding) and payment processing, the risk of inaccurate global bank master data is more definite, thereby causing risk in your payment screening processes. If the bank master data being screened is inaccurate, then most assuredly your risk management program is not in compliance.

Don't wait for a problem in the FI or corporate payments processes – this encompasses data capture at onboarding, bank master data validation and enrichment at the time of making a payment and when screening payments messages. Consider implementing a solution to automatically validate global bank master data accuracy and enrich data throughout the front-to-end payments process, thereby also reducing risk in your payments screening compliance processes.

Leslie Bailey
Vice president of financial crime compliance and payments
LexisNexis® Risk Solutions

Conclusion

As more companies embrace digital transformation, business automation is changing how FIs and corporates leverage the power of data-driven ERP platforms. Digital payments, when managed effectively, have the power to improve customer experiences and business futures. A streamlined digital payments process will help make consumer, FI and corporate transactions modern, uncomplicated and value-focused.

The
2022 Digital Payments Guide
For Corporate Payments

PYMNTS.com | LexisNexis RISK SOLUTIONS

About

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about “What’s Next” in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

LexisNexis® RISK SOLUTIONS

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

All information, data, charts, graphs, figures and diagrams contained herein are for informational purposes only and not intended to and shall not be used as legal advice. LexisNexis Risk Solutions assumes no responsibility for any error or omission that may appear in this document.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe, please email us at feedback@pymnts.com.

DISCLAIMER