

Future *Forward*  
**Momentum**



# Contents

- 1** An introduction from George Doolittle
- 3** Reinventing correspondent banking
- 8** Global economic outlook
- 12** To combat cyberattacks, SWIFT launches mandatory security standards for members
- 16** Data in high fidelity
- 23** Peeking behind the curtain: The meaning of payments
- 30** SWIFT global payment innovation initiative: Innovation through collaboration
- 34** The foreign exchange market in 2017: About-face!
- 38** The rise of RegTech
- 42** Banks embracing APIs to improve — and expand — their customer relationships
- 46** Partnering to protect the client experience



## George Doolittle

Executive Vice President  
and Head of Global  
Payment Services

*“I am delighted to share with you this year’s edition of Momentum magazine.”*

*Momentum* focuses on the payments industry and the current challenges, risks, and opportunities facing global banks and nonbank financial institutions. We address topics that have emerged through our Global Payment Advisory Group (GPAG), a team of industry leaders from premier international financial institutions that regularly meet to discuss important topics and issues affecting the transaction banking industry such as innovation, APIs and Fintech, regulation, and fraud and cybersecurity. Since its founding, this group has grown significantly in size and nurtures a vibrant dialogue among payment professionals globally. Today, more than 475 financial institutions in over 85 countries participate in GPAG.

This year, our *Momentum* theme is “Future Forward.” “Future Forward” means coming together with our customers and partners to accelerate seizing real opportunities for global growth. Through collaboration, innovation, and connection, we can inspire and challenge each other — to exceed customer expectations and achieve success together in this ever-changing financial landscape. Reflecting on my 30 years in the banking industry, I have seen the evolution of how we transact, communicate, and deliver services to our customers, and I am seeing a paradigm shift in correspondent banking as our industry becomes more affected by the political and regulatory environment. However, I strongly believe that there has never been a better time to come together as a community, and that collaboration is critical to serving our customers with transparent and simple services. The *future* is now and ours to shape.

We hope that you find the topics and perspectives presented within these articles interesting and beneficial. We look forward to collaborating with you on “Future Forward” solutions and sharing best practices to better our industry.

As always, we are grateful for your partnership and the business you entrust with us.

Thank you and enjoy the 2017 edition.

A photograph of a modern office environment. In the foreground, a man in a grey suit and glasses and a woman in a grey blazer are looking at a laptop. In the background, other people are working at desks. A semi-transparent graphic with a red-to-yellow gradient is overlaid on the bottom half of the image.

Future *Forward*  
Insights



## Reinventing correspondent banking

Forward by George Doolittle

*Correspondent banking is an essential component of the global payment system, especially for cross-border transactions. Through correspondent banking relationships, banks can access financial services in different jurisdictions and provide cross-border payment services to their customers, supporting, inter alia, international trade and financial inclusion.*

*Until recently, banks have maintained a broad network of correspondent relationships. But, there are growing indications that this situation might be changing. In particular, some banks providing these services are cutting back the number of relationships they maintain.*

Correspondent banking is one of those oldest professions in the world of finance, so some say. Maybe this is the reason why there is such a clamor about its impending death or, maybe, antipathy is just in fashion. Anyway, I thought I would share some of my thoughts on the future of correspondent banking. Readers may be disappointed because I am less concerned with the impact of technology on the business and more concerned about politics, regulations, transparency, and customer expectations.

Cross-border correspondent banking and domestic correspondent banking were born of two necessities: To enable commerce and to enable travel.

During the period of the emergence of nation-states and city-states, when travel was by foot, horse, or sea, identity and creditworthiness were difficult to ascertain. Banks eventually relied on the expertise of local bankers as proxies to deliver services to their indigenous customers.

I started my career with a bank founded to serve Philadelphia's merchants, when the city was the East Coast hub of trade with China and trade in wool and hides. The bank thrived because of correspondent banking. By the time I joined the bank — almost 20 years later — we were still chasing trade transactions. U.S. dollar check clearing had been added to the correspondent business in the late 1950s as U.S. dollar check followed post-war U.S. interests around the world. We were actively promoting our trade, check, and wire capabilities, and the financing therein. The global contacts soon led to financing

correspondent banks (including working capital) and eventually to sovereigns and the balance of payments financing.

The themes remained the same though: Banks at a national and local level leveraging each other's native knowledge to enable commerce and travel. There were hiccups here and there, as banks stretched the core and went outside their skill set (thus the sovereign credit crisis). Meanwhile, technology began to ease the work of processing departments (all those papers and cards) and deal makers with the advent of the computer. On the network front, banks came together in the 1970s to create SWIFT and check single bank solutions. Investment in this new capability was socialized in the financial community and the community lent — pro bono — subject matter experts to assist in the development of the capability.



SWIFT evolved from wires and reporting to securities and custody as banks spread across the planet following globalization and rise of MNCs (multinational corporations).

Correspondent banking gathered momentum with:

- The rise of the MNC
- The development of equity and debt markets
- The growing ease of travel
- A benign regulatory environment
- New technology
- The rise of global banks
- The expanding role of the U.S. dollar

We will come back to some of these developments later, but first I am going to fast forward to today and, most importantly, the emerging political and economic trends sowing the seeds of renewal in correspondent banking.

I believe that correspondent banking is beginning a process of reinvention as the solution to commercial services, mobility (immigration, study, and labor), financing, and support settlement for markets for some very simple reasons:

- The rise of regulatory nationalism, protectionism, and populism
- Regulatory activism of all colors
- The return home of the MNCs now faced with local competition enabled with technology and education
- The waning of the global banks
- Emerging processing and payment technologies and digitalization
- A multicolored approach to even the barest, most simple infrastructure and regulation (e.g., ISO 20022)
- The rise of financial crime and the possibility of state-sponsored global corruption





Banks are again faced with the byzantine complexity of national rules: Protectionists' trade policies and the rise of political currencies. As elements of globalization reverse, transaction costs, fines, and penalties are multiplying not only in value but also in complexity driven by national prerogatives. The ratio of human resources, legal, audit, and compliance to customer-facing teams is multiplying. National banking legislation and rules are measured in thousands of pages versus hundreds a decade ago. Even areas of technological change, which underpin globalization (e.g., ISO20022), are spawning a range of colors rather than a global solution for payments.

Therefore, correspondent banking is reinventing itself, drawing on experience and new technology. Banks are refocusing on the value local and national banks can provide, while looking for efficiencies and solutions on existing networks to compete with new players. Overall, correspondent banking can deliver the same or better in terms of cross-border solutions as newer players emerge. But, wrinkles have to be ironed out, which is the goal of new efforts such as SWIFT gpi. Moreover, the banks' version will square with national rules, and leverage platforms that also service the polity and local needs, such as financing homes, development, and education.

What will be critical, though, is that solutions:

- Are made available to as many banks as possible
- Are transparent in regard to processing and pricing
- Are predictable, trackable, and connected to mobile solutions domestically
- Exceed expectations and are priced reasonably, including compliance and adherence to local rules
- Provide E2E experience
- Leverage emerging technology where it makes sense
- Recognize that identity and related data are private and should be protected
- Are committed to their communities

The future for correspondent banking — in my opinion — looks bright. ■

A man and a woman in business attire are engaged in a conversation in what appears to be a market or construction site. The woman, on the left, has short dark hair and is wearing a blue sleeveless top and a pearl necklace. The man, on the right, is wearing a light blue shirt and a red tie, and is holding a smartphone. The background shows a wooden structure and various items, suggesting an outdoor or semi-outdoor setting. A semi-transparent yellow and orange gradient bar is overlaid across the middle of the image, containing the text.

Future *Forward*  
Guidance



## Global economic outlook

The global economy has moved on to greener pastures this year after 2016 registered the slowest pace of economic growth since 2009. Encouragingly, the improvement has been broad-based, as many of the world's advanced and developing economies have seen an uptick in economic activity thus far in 2017. We expect global economic growth to maintain this faster pace, but a return to the supercharged growth rates experienced during the peak of the last expansion is unlikely as tighter monetary policy and secular challenges limit the extent of any further acceleration.

In the United States, economic growth averaged roughly 2% in the first half of the year. Although this growth rate is perhaps disappointing to some after the surge in optimism following last fall's presidential election, 2% still marks an improvement from last year's 1.5% pace. Business investment has been the key driver of faster growth this year.

Businesses have ratcheted up their spending on equipment and structures as commodity prices have stabilized and labor has grown increasingly scarce. We look for full-year 2017 real GDP growth to register 2.1% in 2017 before picking up to 2.5% in 2018.

*“Despite the pick-up in economic activity across the English Channel, the UK is one of the few major advanced economies seeing slower growth this year compared to 2016.”*

Across the Atlantic, economic growth rates in the eurozone and United Kingdom have diverged. The eurozone has seen its recovery become increasingly self-sustaining amid steady employment gains and improving business sentiment. Despite the firming growth environment, eurozone monetary policymakers face a challenging conundrum; the unemployment rate has reached an eight-year low, but core inflation has been listless around 1% for the past two years. Our current forecast looks for real GDP in the eurozone to grow 2.1% in 2017 which, if realized, would be the strongest annual average growth rate since 2007. We believe improving economic conditions and gradually accelerating prices will spur the European Central Bank to continue tapering its bond purchases in the months ahead and cease buying bonds altogether in the first half of next year.

Despite the pick-up in economic activity across the English Channel, the UK is one of the few major advanced economies seeing slower growth this year compared to 2016. In the wake of last year's Brexit referendum vote, sterling depreciated dramatically. This

in turn has led to a surge in inflation above the 2% target set by the Bank of England. This rapid inflation, coupled with stagnant wage growth, has weighed on growth in real disposable income and exerted headwinds on consumer spending growth. We expect real GDP growth to strengthen modestly in 2018 as inflationary pressures begin to subside later this year and UK exporters take advantage of stronger growth around the world, particularly in the eurozone. That said, the ongoing negotiations related to Brexit will continue to loom over the UK economy over the next few years, representing a major downside risk moving at a glacial pace in the background.

Volatility rose sharply in many financial markets in early 2016 as investors fretted that growth in the Chinese economy was slowing sharply. Fast forward six quarters, and Chinese economic growth has been remarkably stable between 6.5% and 7% over that period. The government “encouraged” stronger credit growth last year when the economy needed an extra boost, and it appears that policymakers are now attempting to tamp down credit growth so as not to inflate a housing bubble.

We forecast that real GDP growth in China will slow somewhat in 2018 relative to the rate that likely will be achieved this year. Although there is justified concern about the amount of financial leverage in the nonfinancial corporate (NFC) sector, we believe that the Chinese government should generally be able to manage any nonperforming loan issues that may arise in the banking system in the foreseeable future.

However, China also faces some fundamental issues that likely will lead to even slower economic growth in the next decade. Not only will the working-age population in China decline in coming years, but the build-up in leverage in the NFC sector likely will constrain growth in capital spending.

Elsewhere, the Japanese and Canadian economies have accelerated to multi-year highs on a year-ago basis, and Brazil and Russia have continued their long journeys back from severe recessions. On balance, faster growth has taken root in many of the world's economies. We forecast that global GDP growth will pick up from the 3% rate registered in 2016 to 3.4% this year and next. Despite the acceleration, a return to the growth rates of 5%-plus that prevailed in the mid-2000s seems unlikely. Removing some of the extraordinary monetary stimulus that has been in place in recent years will make financial conditions somewhat less accommodative. Furthermore, aging populations are weighing on economic growth in many of the world's economies, and not just in the developed nations. China and Russia, for instance, will both grapple with secular declines in their labor forces in the years ahead.

The improved economic outlook has driven a reversal in the direction of monetary policy around the world. Although the pace of change will likely be quite gradual, monetary policy has begun to shift toward less accommodation after the past few years saw increasingly more policy

accommodation. The Federal Reserve, the European Central Bank, the Bank of England, and others all appear poised to tighten policy to varying degrees over the next 18 months. By historical standards, monetary policy will likely remain relatively easy in many countries, but this is consistent with the downshift in growth and inflation compared to past expansions. Even if the shift is a gradual one, central bank convergence toward tighter policy marks an important inflection point in this expansion, and with it comes both new opportunities and risks. ■



A professional office scene featuring a man with a beard and mustache, wearing a white dress shirt and a blue and black striped tie. He is smiling warmly at a woman whose back is to the camera. She is wearing a light blue blazer. They are seated at a desk with a white coffee cup and some papers. The background shows a window with a view of greenery. A semi-transparent yellow and orange gradient bar is overlaid across the middle of the image, containing the text.

Future *Forward*  
Insights



## To combat cyberattacks, SWIFT launches mandatory security standards for members

**New requirements designed to tighten controls at local access points**

The media pointed an unwelcome spotlight on SWIFT, the global banking platform, in 2016. First, hackers attempted to steal \$951 million from Bangladesh's central bank account at the Federal Reserve Bank in New York (FRBNY). While FRBNY blocked \$850 million in transactions and recovered \$38 million, investigators later discovered similar cyberattacks targeting SWIFT member-banks in Vietnam, the Philippines, and other nations across Asia, Europe, and even the U.S.<sup>1,2</sup>

While attacks never compromised the SWIFT network, they exposed a growing threat: Sophisticated schemes that target vulnerabilities at member banks. In several cases, hackers were alleged to have deployed malware targeted at a specific bank to gain access to the bank's system that accessed the

SWIFT network. The hackers then inserted unauthorized payment orders into the bank's system and sent the payment orders through the SWIFT network, which subsequently authenticated them as payment orders initiated by the banks.

## Increased vigilance will help protect SWIFT members

Targeted cyberattacks are on the rise globally across all industries. In 2016, the Ponemon Institute reported that three out of four data breaches were caused by malicious or criminal attacks from outside the organization, or by negligent employees or contractors.<sup>3</sup>

As previously discussed in our [Momentum article, “Is SWIFT still secure?”](#) any collaborative network is only as strong as its weakest link. In that spirit, SWIFT introduced new network requirements for all members as part of its Customer Security Programme (CSP). Across 200 countries, more than 11,000 banking and securities companies, third parties, and corporate customers of SWIFT must comply with the CSP.

## A Customer Security Programme overview

SWIFT published its final CSP standards at the end of March 2017. The [CSP framework](#) includes 16 mandatory controls and 11 advisory controls. During 2017, SWIFT members will need to demonstrate their compliance with the mandatory controls through a self-attestation process. Requirements apply to direct members as well as those who connect via service bureaus.

In January 2018, SWIFT will begin more formal inspections and enforcement, and will make each organization’s compliance status visible to other network members. Penalties for noncompliance are still in development.

The CSP framework will help banks focus on three objectives:

1. Secure their environment
2. Know and limit access
3. Detect and respond

Within these three core components, mandatory requirements include:

- Promptly installing security patches on user computers
- Using multifactor authentication for SWIFT-related applications
- Installing malware protection software
- Conducting integrity checks at regular intervals on any database that records SWIFT messages
- Developing an incident response plan

SWIFT designed the CSP standards to reduce potential vulnerabilities and strengthen security across each member-bank’s infrastructure, to prevent a hack of the member-bank’s system. SWIFT also aims to ensure that each member-bank has processes to monitor, detect, and, if necessary, quickly respond to anomalous activity within its own network. Prompt information sharing is critical to protect all SWIFT members.

*“Targeted cyberattacks are on the rise globally across all industries.”*

## Additional resources and guidance available

While every SWIFT member will need to address its own environment, Wells Fargo has developed a comprehensive and actionable incident response program to provide assistance in the recovery process if a security breach occurs.

Automated alerts are another tool that can aid banks in compliance and transaction security. Banks can set specific alerts for their SWIFT-connected accounts, such as transaction amount, type, or on and off

hours activity. Any activity outside these parameters can trigger a real-time alert to web or email-enabled mobile devices. This helps automate fraud monitoring by the sending bank and assists in early detection.

SWIFT members can consult with their banking partners through this process to adhere to the CSP requirements, including the advisory controls. These best practices will help improve transparency across the network and help the industry take a proactive — rather than reactive — approach to security. ■

1. CNN Tech, "Banks urged to tighten security as hacks continue," August 31, 2016.

2. CSO / IDG News Service, "Up to a dozen banks are reportedly investigating potential SWIFT breaches," May 27, 2016.

3. Ponemon Institute, "2016 Cost of Data Breach Study," June 2016.

## Components of SWIFT's new security standards

### Secure your environment



1. Restrict internet access
2. Segregate critical systems from general IT environment
3. Reduce attack surface and vulnerabilities
4. Physically secure the environment

### Know and limit access



5. Prevent compromise of credentials
6. Manage identities and segregate privileges

### Detect and respond



7. Detect anomalous activity to system or transaction records
8. Plan for incident response and information sharing

Source: SWIFT

A woman with dark hair, wearing a white tank top, is looking towards a man in a suit who is out of focus in the foreground. The background is a bright, blurred outdoor setting. A large, colorful abstract overlay in shades of yellow, orange, and red is positioned in the lower-left and center of the image, partially covering the text.

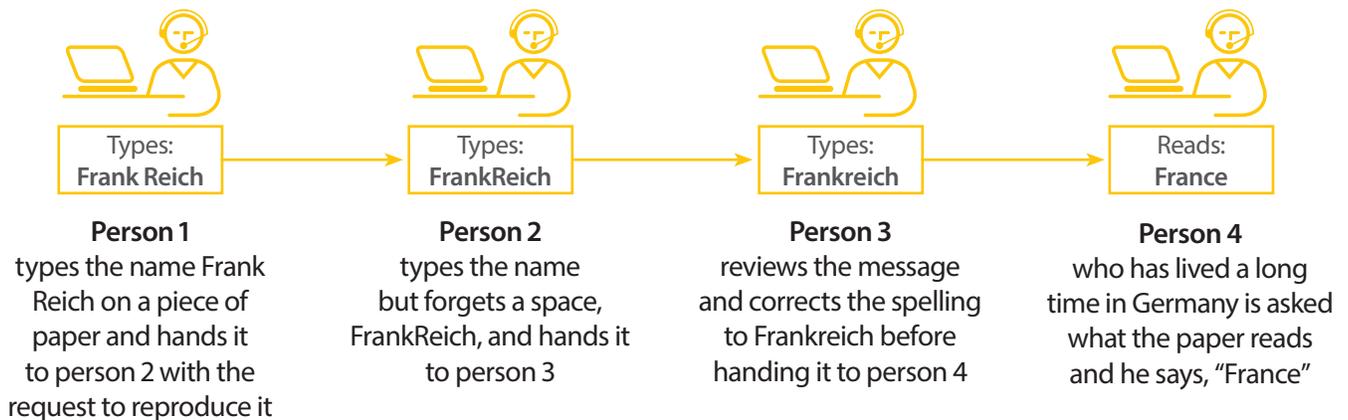
Future *Forward*  
Guidance



## Data in high fidelity

Data quality has become a hot topic in payments. Partially driven by compliance needs but also big data projects, the request for highly accurate data is increasing. Data fidelity means that as data travels from the point of origination to consumption, it retains its granularity and meaning. While format might change for data in transit, the goal is to ensure that its meaning remains unaltered.

To illustrate the issue, consider the following scenario:



The issue here is the data was transmitted in free format text, and none of the processors (people in this case) had any context what the data element was supposed to mean. Differentiating geographic names from company and individual names is especially critical in sanctions screening and anti-money laundering (AML). Differentiating between whether Cuba is a country or a first name is important.

Let's explore in more detail recent industry developments and discussions around party fields in payment orders.

### Finding your place in the world

In the absence of a globally unique identification scheme (for legal entities, it is emerging as the LEI), the traditional way to identify an individual or legal entity is by:

- **Name.** For individuals, first name, last name
- **Street address.** Comprised of dwelling identifier (e.g., apartment number), building number, and street name. In some jurisdictions, a PO box is acceptable, or a building might have a unique name.
- **City and postal code**
- **Country**

Another mechanism to identify a location is latitude and longitude, which GPS systems and phones use. While these are great for identifying a place on earth in the two-dimensional space, no clear standards exist to identify a specific dwelling in a multistory or tenant building.

### The free format trap

Ideally, you should identify all key data elements separately and avoid concatenations. This starts with the name. Having clarity on what the first and last names are will make it easier to differentiate between Frank Madison and Madison Frank. However, having dedicated fields will increase the size of the underlying message. This is probably the best explanation of why in the initial design of SWIFT messages, the name and address field did not have any specific format or subfields. Free format text provided the most flexible way to accommodate various name and address formats and sizes. This is especially relevant in the case of limited field sizes, such as in the ordering party and beneficiary field in traditional SWIFT messages. The downside is that it can be more ambiguous and difficult to validate if not all the required information is present.



## The dreaded F option

Heightened regulatory scrutiny has motivated the payments community to address the issue by eliminating the free format option in 2020. The industry will need to move to a more structured address format such as Field 50F and 59F. Field 50A and 59A will still be appropriate when the ordering customer or beneficiary is a corporation with a nonfinancial institution Business Identifier Code (BIC) assigned to it. In most cases, however, parties will not have BIC identifiers, and the F option will need to be used. The recommended<sup>1</sup> use is:

Subfield 1 'Party Identifier'	/(Account) or (Code) (Country Code) (Identifier)
Subfield 2 'Name and Address'	1/Name of the ordering customer 2/Address details 3/Country code/Town

The relevant aspects of these subfields are:

- Dedicated subfields for name, address (e.g., street and building), and town and country
- Use of the ISO country in subfield 3
- Other code options for identification numbers, and date and place of birth

For now, the size of the party field is not changing, and you still need to accommodate the relevant information in 4x35 characters. It will be important to decide how name and address information is populated when the line size is not sufficient (example: name or address is longer than 35 characters). In these cases, the subfield tag can be repeated in another line. For more technical details, please review the PMPG market practice guidelines and the BAFT Best Practices and Guidance: Formatting Payments and Handling Inquiries Related to FATF Recommendation 16.<sup>2</sup>

The payments industry is contemplating an expansion of the party fields, either in the number of lines or the length of each line to accommodate longer names and avoid truncation issues. Payments on behalf of (POBO) and receiving on behalf of (ROBO) create further challenges, as traditional MT 103 messages do not have fields for ultimate debtor and creditor parties, increasing the need for either additional fields or more lines in existing party fields.

*“Heightened regulatory scrutiny has motivated the payments community to address the issue by eliminating the free format option in 2020.”*

## The party is on ISO 20022

Looking into the future, the industry needs to consider the upcoming adoption of ISO 20022 in the correspondent banking space. Granularity of party fields will need to be discussed in this context once more.

For example, in ISO 20022, the structured option to represent parties has a name field of 140 characters, and very detailed subfields for the address data:

- StreetName
- BuildingNumber
- PostCode
- TownName
- CountrySubDivision (e.g., states, cantons, provinces)
- Country

While the F option provides a subfield for town and country postal codes, states, provinces, and building numbers were not tagged specifically. It would be ideal to have separate fields for first and last name. ISO 20022 has a field to label an address as residential versus business, so that might help as well.

At this time, it is not known when the industry will switch to ISO 20022 for interbank payment orders, but many local payment systems have already embarked on the journey. The U.S., Canada, and eurozone have firm plans to migrate to the new format, and Switzerland and Japan have already migrated. By 2022, the majority of high-value payments will be settled via ISO 20022 compliant payment system.<sup>3</sup>



## Where do we go from here?

While domestic requirements on name and address information will vary in the international context, we are on a path for more granularity. To position an organization for these changes, it's best to implement the most granular data format so that it is easier to generate other less stringent formats. Going from ISO 20022 address fields to the F option in MT messages will be easier than starting with a free format field.

ISO 20022 structure	F option structure	Free format
<Nm>FRANK REICH</Nm> <PstlAdr> <StrtNm>125TH ST</StrtNm> <BldgNb>115</BldgNb> <PstCd>10027</PstCd> <TwnNm>New York</TwnNm> <CtrySubDvsn>NY</CtrySubDvsn> <Ctry>US</Ctry> </PstlAdr	1/FRANK REICH 2/115 125 TH ST 3/US/NEW YORK, NY 10027	FRANK REICH 115 125 TH St NEW YORK, NY 10017 AMERIKA

The first step in this endeavor is to inventory all existing sources of payment party data and identify which systems house the gold copy of such information. For beneficiary details, this will in most cases be the customer. If the customer is using a bank-owned interface such as an electronic banking system, then this needs to be modified to capture structured address data, if they still allow unstructured data. In the event that payment files are received from a customer's enterprise resource planning (ERP) system, then this change will not be just dependent on the bank's system, but the corporate customer and its vendor will also need to adjust their payment output formats.

It is also recommended that cross-border payments use the ISO country codes in the beneficiary and ordering party field.

In electronic banking systems, it might be best to provide country code selection lists for the user.

When populating Field 50 and 59, if the content exceeds the available space, then follow the earlier referenced guidelines provided by BAFT and PMPG.

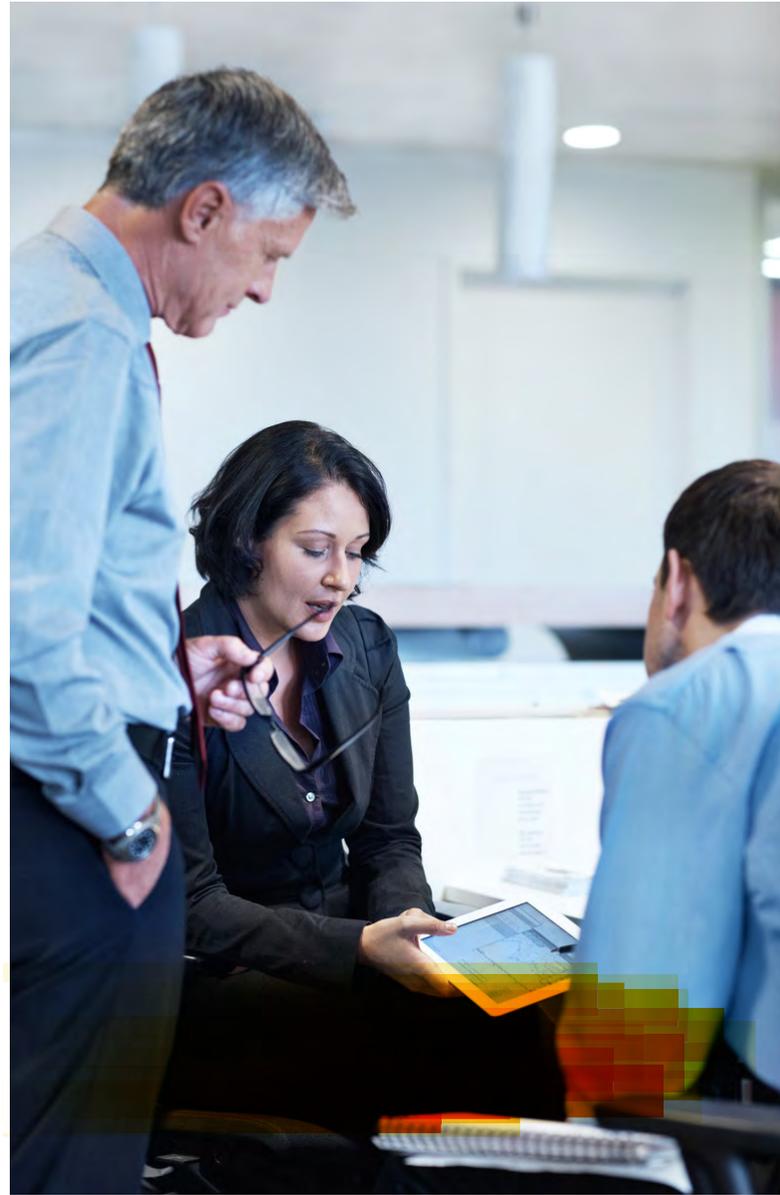
*“Going from ISO 20022 address fields to the F option in MT messages will be easier than starting with a free format field.”*

Some countries do not like PO boxes in payment party messages, and it will be best to ensure full street addresses are available. This recommendation will be easier to address in the ordering party field, but might be more difficult to accommodate in the beneficiary field.

You will need to supplement all these technical changes and requirements with a customer education campaign. Some end-user customers might not be willing to update their internal databases and systems, but it will be important to point out the benefits, such as avoiding delays in payment execution and investigation fees.

## Conclusion

The year 2020 might sound like the industry has plenty of time to adjust to these changes, but this is not the case. The scope of the changes and number of systems affected might vary by bank, but in most cases, this will be a multiyear effort when you consider required testing and customer engagement. Preparation needs to start now in 2017, to gather the overall requirements and put budgets in place for 2018 and 2019. ■



1. PMPG Market Practice Guidelines for use of fields 50a Ordering Customer and 59a Beneficiary Customer to comply with FATF Recommendation 16 (<https://www.swift.com/about-us/community/swift-advisory-groups/payments-market-practice-group>)
2. <https://www.baft.org/events/general/2016/09/20/baft-releases-fatf-guidance-for-wire-transfers>
3. A detailed map of global ISO 20022 payments initiatives is available at: [https://www.iso20022.org/documents/adoption/Introduction\\_maps.ppt](https://www.iso20022.org/documents/adoption/Introduction_maps.ppt)



Future *Forward*  
Partnerships



## Peeking behind the curtain: The meaning of payments

Processing a payment for banks used to be all about getting the instruction to the next party in the payment chain. Straight-through processing (STP) was synonymous with not touching the payment in your own shop regardless if the payment was causing issues downstream at other banks. Over the years, this model has changed due to increased regulation and compliance requirements, and just knowing debit and credit parties and amounts is not sufficient. Anti-money laundering (AML) analysis requires banks to understand transactions and country flows. Data quality in all fields of the payment order becomes paramount.

Two segments of a payment order have been subject to increased scrutiny: Ordering Party and Beneficiary (debtor and creditor in ISO 20022 terminology) and the purpose of the payment. However, while party details are

subject to specific international regularity recommendations such as FATF 16, the purpose of payments discussion has been mainly a concern for local regulators without much international compatibility discussion.

This paper primarily focuses on the current state of the purpose of payment codes and their challenges in the international payments environment. In particular, we will look at the challenges in the current MT messages and the efforts of the industry to standardize them. Special consideration will be given to the upcoming ISO 20002 migration and the impact on interoperability.

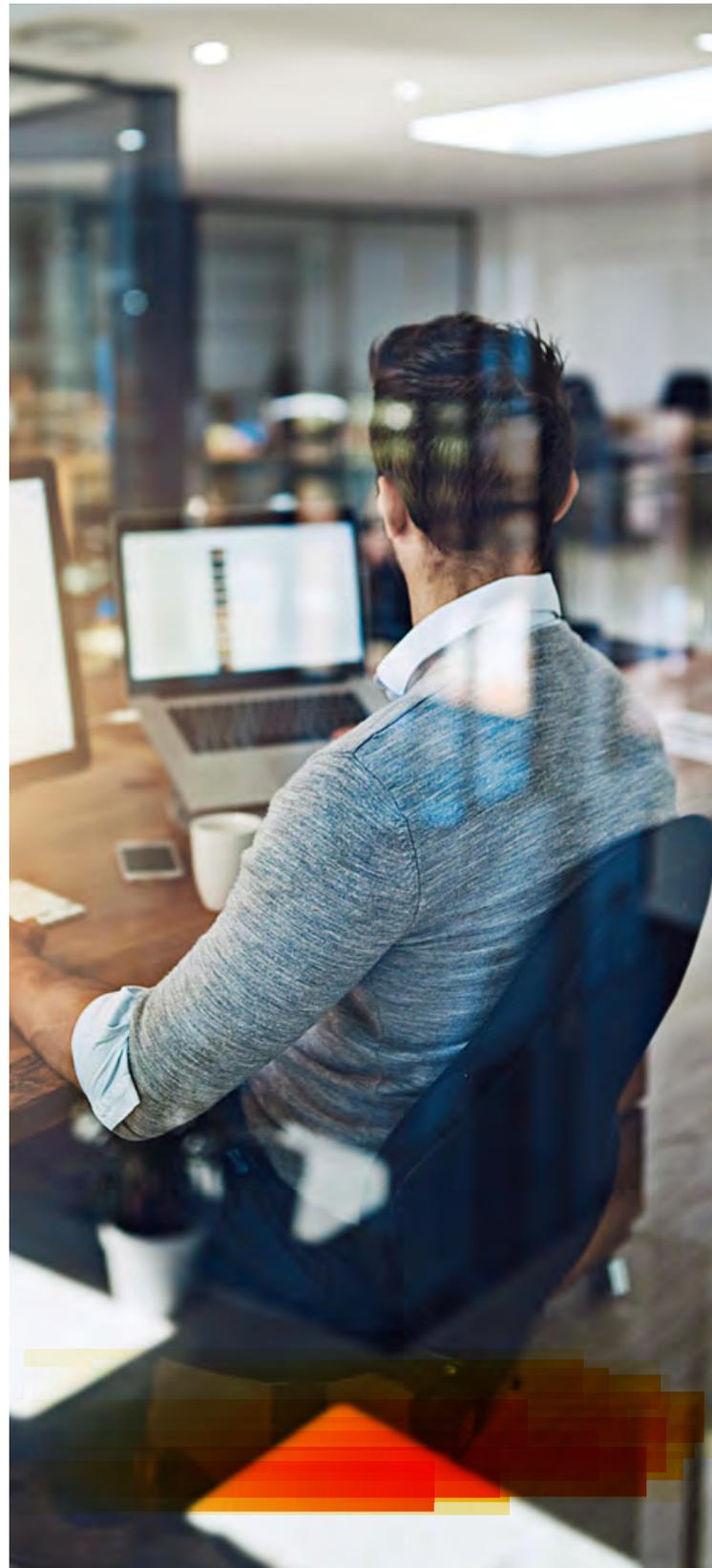
### **Purpose of payment codes**

While payment purpose codes are nothing new and have been in existence since the last century to support central bank reporting requirements, their use has initially been declining. However, they are getting a new life as some markets like China and India have introduced new requirements for their use. As their definition and use are driven by various local regulators, no standard exists. For example: South Africa uses a five-digit numeric code while China has implemented a five-character alphanumeric version. Definitions vary, and are overlapping in some cases. Jordan has a purpose code 0801 for Telecommunication Services, 0803 for Information Technology Services, and 0807 for Marketing and Media Services. Selecting the right code for “storing videos in a cloud-based service” becomes a real challenge in this case.

The examples above illustrate how difficult it is for the ordering party to select the right code and for the regulators to have assurance that the codes being used provide high-quality data. Let's look at key aspects of data quality:

Issues with data quality:

**Completeness:** Data are missing or unusable



**Conformity:** Data are stored/transported in nonstandard format

**Consistency:** Data values give conflicting information

**Accuracy:** Data are incorrect or out of date

And apply it to POP codes:

Data quality attribute	Relevance to POP codes	Current issue
Completeness	Is the user in possession of the various codes?	As POP codes are very local, the ordering party will, in most cases, struggle with obtaining the relevant code list.
Conformity	Can the code be transported with consistency in different payment message types?	As we will see in the next section, this is really the biggest issue between message types.
Consistency	Can codes be used across countries in a consistent manner?	As code lists are local, conflicts can arise if regulators from the sender and beneficiary country have different code requirements.
Accuracy	Do all parties have access to the most recent code list and is the right code being used?	The sender will have difficulty knowing if the codes are correct and the most current.

So, who owns the accuracy of the purpose of payment codes? The sender initiates the payment and should know what class of services is being paid for; however, the lack of standards makes it difficult for the sender to comply and they would need to rely on the beneficiary to advise the correct code. But from an accuracy perspective, that might be problematic if the wrong code is communicated. For financial transactions, the sender is probably best suited to determine the right code.

### Fit for purpose and existing standards

As highlighted in the table above, the challenge is to decide. Which field should one use for payment purpose codes in cross-border transactions? Should the code be populated in field 26T, 77B, 70, or even field 72? The answer to this question varies and depends on the geography of the payment parties. In some markets, 26T is not supported by local banks; hence, a generic field such as field 72 is recommended, which runs counter to efforts in other markets that would like to restrict the use of this free format field.

### Field 26T MT103

The definition of this field stipulates that it should be used to identify “the nature of, purpose of, and/or reason for the individual transaction; for example, salaries, pensions, dividends” and a three-character code can be used. While the field definition is describing the purpose of the payment, what is interesting to note is that most of the codes that local regulatory agencies have defined are longer than three characters (UAE has three). In some cases, the purpose of payment is a free text description. Also, the current three characters do not allow referring to a specific issue of a code list. In summary, the existing field 26T is not adequate to house the payment purpose codes in use.

Most markets have hence selected a free format field 70 or 72 to include the purpose of payment code.

### Field 77B MT103

The regulatory reporting field provides more options as it is more general and allows for “regulatory information required by the authorities in the country of receiver or sender.” However, restricting the use to the sender and receiver is misleading as in most cases, the purpose of payment needs to be advised to authorities in the country of the beneficiary or ordering customer (or bank). The field size at least of 3 x 35 characters makes this field more suitable for purpose of payment codes as it can capture multiple codes and country codes.

In some markets, 77B is not supported by local banks; hence, a generic field such as field 72 is recommended, which runs counter

to efforts in other markets that would like to restrict the use of this free format field.

### MT202

The MT202 does not offer field 26T or 77B; hence, users need to place payment purpose related information in field 72.

### ISO 20022 external code list

In pain and pacs messages, a field purpose (< purp > cd >) in the CreditTransferTransactionInformation < cdtrftxinf > segment references an external code list (ExternalPurpose1Code), which contains 162 purpose of payment codes covering various aspects of payment transactions. As this is an external codes list, maintenance can be done quarterly if codes need to be added. The codes contain a definition but do not follow a consistent taxonomy. More work will need to be done to ensure the industry has a more consistent framework in assigning these codes.

Agreeing on a standard list of codes and definitions will make it easier for users to pick the right code and manage against a complete list. The standard list would also

*“Agreeing on a standard list of codes and definitions will make it easier for users to pick the right code and manage against a complete list.”*

enable local regulators to map against the global list and identify gaps that then can be added to the external codes list.

### Reality in the field

Lack of guidance by the global community and absence of standardization have led local regulators to come up with their own recommendations and requirements where codes are to be placed. The current unstructured approach leads to an increase in inquiries and payment delays.

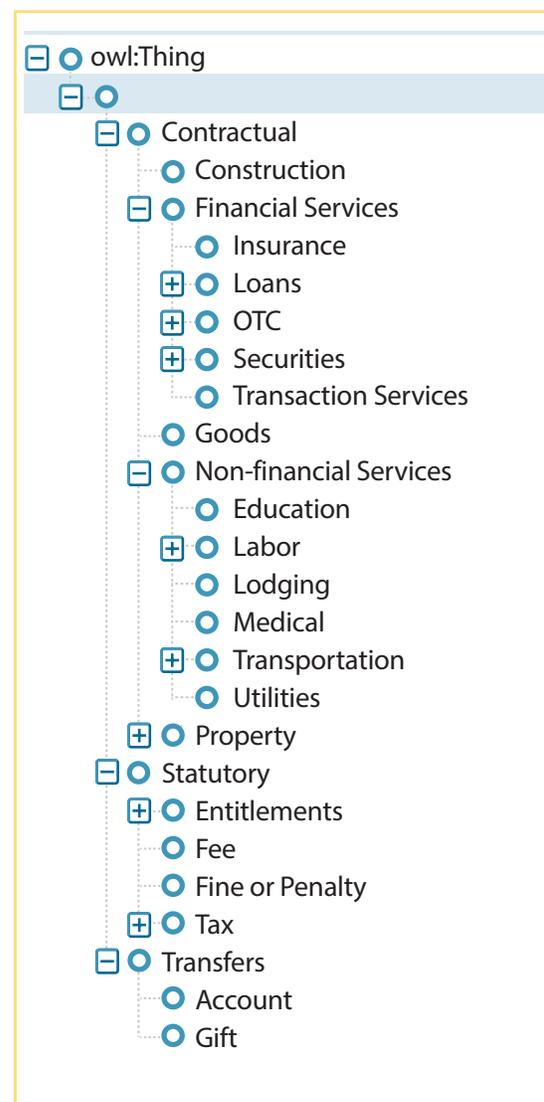
More countries are adding requirements around purpose of payment information. Recently, Cambodia announced the requirement to include the purpose of a payment.

### Search for the missing payment purpose codes: Semantic model

Having a standard code list is a start, but gaps exist. For example, codes are in place to advise that a payment relates to transportation by Air, Railway, Bus, or Ferry but no codes exist for truck or vessel. Some codes are very granular, like differentiating between an E-Purse Top Up and a Mobile Top Up, while others are broad, like Costs.

While these cases have been developed with the input from different communities, it would be good to look at this from an overall standardization perspective that keeps these codes at the same level of granularity, or introduces a hierarchy to them (like the service codes in the BankServicesBillingStatement message). From a standards perspective, this is desirable but also a significant task. The

chart on the right provides an illustration of this approach by establishing categories and a hierarchy. Well-defined categories with adequate descriptions and code descriptions should make it easier for communities to map local codes and decide if the global codes are sufficient for their needs or identify gaps that should then be closed through the regular quarterly maintenance process of external codes list.



Sample Semantic Ontology for Payment Purpose



### How do we map from ISO 20022 to legacy standards?

More RTGs systems are adopting the ISO 20022 standard for payments. Once USD and EUR payment systems have migrated, a large part of value and volume of international wires will be conducted in the ISO 20022 format. However, for cross-border payments, the existing MT messages will still dominate; hence, intermediary banks will be faced with the problem to map incoming ISO 20022 messages into the existing legacy standard. One challenge will be where to map the purpose code field, which exists in Customer Credit Transfer and FI to FI credit Transfer to the correct field in MT103 and MT202 messages. Absent any standard change in the MT messages, a market practice will need to be agreed upon as to how to accomplish this.

Standards development can only provide us with fields, codes, and descriptions but the actual usage will require agreement on market practice. One such practice could be to use the global codes list and require that the mapping to the right local codes should be the responsibility of the beneficiary bank or the beneficiary.

Of course the payment details, as well as the global codes, need to be granular enough to enable the mapping. (Example: Differentiation between resident and nonresident creditor is better done by the creditor agent.)

### Conclusion

Purpose of payment codes need to serve multiple masters in the future. While initially the focus has been on the beneficiary bank country compliance, requirements in the interbank chain to have more insights into what gets paid will require a more globally consistent approach. So far, requirements and standards have been driven locally, but the myriad of codes makes it difficult for the originator of the payment to make the right decision what to use and when. Resulting data quality issues should also be a concern for the authorities requesting the usage of these codes. If the users of these codes want to be able to aggregate payment data domestically and cross border, and use the data for policy decisions with some level of quality assurance, then a more standardized approach should be promoted. ■

A photograph of a group of people in a meeting. In the foreground, a woman with long dark hair, wearing a grey cardigan over a black and gold patterned dress, is gesturing with her hands while speaking. To her left, a man with white hair and glasses, wearing a dark suit and tie, is listening intently with his hand on his chin. Another man with brown hair is partially visible on the far left. In the background, other people are seated at tables in a modern, brightly lit room with red and blue seating. The text "Future *Forward* Collaboration" is overlaid on the image in white, with "Future" and "Collaboration" in a bold sans-serif font and "Forward" in an italicized sans-serif font.

Future *Forward*  
Collaboration



## SWIFT global payment innovation initiative: Innovation through collaboration

The SWIFT global payment innovation (gpi) initiative takes aim at resolving cross-border payment pain points by improving the client experience and helping corporate clients achieve their goals via trusted and heavily regulated bank providers.

What sets SWIFT gpi apart from other payments industry initiatives is that it brings together the global banking network on a common infrastructure and standard. In the short term, it provides a practical, implementable solution with robust security. The long-term strategic vision is to create incremental value, evolve, and innovate. Other industry initiatives cannot easily match gpi's immediate scale and global reach.

The first phase of SWIFT gpi, which addresses cross-border payment speed, fee deduction transparency, tracking, and unaltered remittance data, went live in February 2017 via collaboration between global banks and an SLA rule book. In May, SWIFT launched the gpi tracker to provide payment tracking and fee deduction transparency throughout the gpi credit transfer chain to the gpi parties involved in the payment.

SWIFT also delivered the gpi Observer Insights in April to monitor and enforce gpi member-bank adherence to the gpi SLA rule book. The April version of Observer Insights reports on speed of payment availability and timeliness of payment status updates. SWIFT has targeted June as the rollout date for enhancements to report fee deductions and unaltered remittance data. The standalone gpi directory that catalogs live gpi participants, the currencies they support, and their currency cutoff times is scheduled to be available in the third quarter of 2017.

SWIFT has created and is facilitating a vision group to manage the medium- to longer-term strategic evolution of the cross-border payment space that complements phase one. The vision group has prioritized some medium- and longer-term objectives, such as providing incremental value to business-to-business (B2B) payments by providing tools to prevent exceptions as well as to better manage certain types of exceptions. Enhancing liquidity management and enabling payments digitalization with rich remittance data are two other medium-term enhancements planned for the gpi infrastructure. The vision group continues to discuss expanding gpi to cover other business needs and service levels as the infrastructure evolves, while providing value in the medium term.

In parallel, the group is exploring longer-term strategies, such as new technologies like blockchain and distributed ledger (DL) technology, application programming interfaces (APIs), artificial intelligence (AI),

## SWIFT gpi by the numbers

**100+**

Members strong

**224+**

Countries represented

**75%**

Of SWIFT network traffic

**21**

Successful pilots

**22**

Banks live

**65**

Country corridors covered

Source: SWIFT.com

and new clearing and settlement models. SWIFT recently announced a gpi proof of concept to better understand the opportunities and challenges with using blockchain or DL technology for nostro reconciliation with a number of gpi member-banks. Phase one of the nostro reconciliation proof of concept starts with six banks testing the concept and an additional 20 banks following phase two.

The payments space is evolving quickly. Developing a centralized infrastructure that enables the banking community to use common requirements — and facilitates global reach, interoperability, and collaboration — while testing new technologies on a scale required to shape the future payments landscape is what makes SWIFT gpi one of the most important payments initiatives today. ■

*Wells Fargo is a member of SWIFT's global payment innovation (gpi) initiative and is implementing steps so it can be live on the infrastructure by the first quarter of 2018.*



A photograph of two men in business suits walking in a city street. The man on the right is older, with grey hair, wearing a dark suit and a purple tie. The man on the left is younger, wearing a dark pinstriped suit and a patterned tie. They are both looking towards the right. In the background, there are tall buildings and a large red flag with a yellow emblem. A semi-transparent yellow and orange gradient bar is overlaid across the middle of the image.

Future *Forward*  
Guidance



## The foreign exchange market in 2017: About-face!

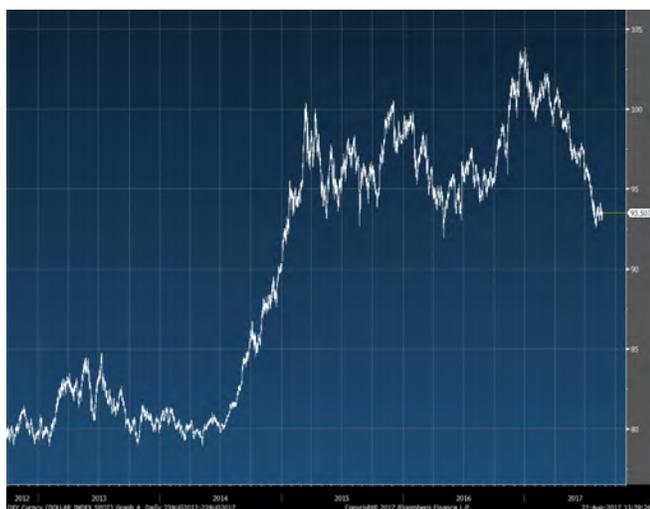
A sea change seems to be taking place in the global currency market. For three years, from late 2013 to 2016, the U.S. dollar was on a largely uninterrupted strengthening trend. During that time, the Dollar Index, a basket index of dollar rates against the currencies of U.S. trading partners, rose over 30%, making U.S. exports more expensive and helping to keep a lid on inflation by holding down import prices.

The dollar's peak occurred right around New Year's Day 2017, after which the trend reversed convincingly. Through August, the Dollar Index has declined more than 10%, and Wells Fargo Securities' foreign exchange forecasts are calling this the early stages of a multiyear downtrend for the dollar.

### The surging dollar

There is a myriad of pressures affecting currency rates, from investment flows to business transactions to influences from local political events and larger global

factors. In the case of the dollar's recent course, the main protagonist has been the U.S. Federal Reserve, with secondary parts played by other central banks in the G7.



*DXY USD Dollar Index; Source: Bloomberg*

The monetary environment of the last few years has been characterized as one of divergence. This refers to, on the one hand, the Fed’s stated intention, and eventual actualization, of a return to a normalized monetary policy — raising short-term interest rates from the near-zero levels they had held since December 2008 and gradually unwinding the portfolio of \$4 trillion of long-term treasuries and mortgages the Fed had accumulated during its so-called “quantitative easing” (QE) policy. The Fed first raised short-term rates in December 2015, raised them again a year later, and twice again so far in 2017.

Meanwhile, on the other hand, the central banks of most U.S. trading partners were following the opposite monetary policy. Short-term interest rates were driven toward zero and even into negative rates in Switzerland, Japan, and the eurozone in an effort to spark bank lending and economic growth. QE efforts proliferated.

Higher interest rates tend to make a currency more desirable, as they both generate a higher yield on cash deposits and indicate a more robust economy for business investment in that country. Often, the expectation of higher rates is as potent, if not more so, than the act itself.

With the U.S. moving toward higher interest rates and the rest of the world moving in the opposite direction, a stronger dollar was practically a given.

Ancillary factors in the global economy tended to support the dollar’s strength. U.S. economic growth, though substandard, nevertheless outpaced much of the rest of the world. In China, authorities engineered a gradual slowdown in economic growth, which in turn negatively impacted the economies of its supplier countries. Commodity prices declined, partly in response to the higher dollar, harming trade values in producer countries like Australia, Mexico, and Canada. In Europe, political uncertainty undermined the British pound and the euro. Similar dynamics in Brazil pushed its currency to record lows.

Finally, the election of Donald Trump in November 2016 occasioned a burst of dollar buying in anticipation of business-friendly fiscal policies that would mesh well with the Fed’s intended withdrawal of monetary stimulus.

*“Rapid market moves are often followed by periods of consolidation.”*

### What changed?

With remarkable suddenness, the market’s perception of divergence was replaced with one of convergence. The Fed, in its public pronouncements, appeared to be easing off the accelerator of interest rate hikes, as persistent low inflation complicated its view on policy tightening. Meanwhile, other central banks, the European Central Bank (ECB) and the Bank of Canada in particular, raised the possibility of following the Fed in normalizing policy. The latter was notably aggressive, signaling a rate hike in June and following through barely a month later, with the market clearly primed for further increases in the months ahead.

As monetary policies changed from diverging to converging paths, the market’s view on the dollar reversed abruptly.

At the same time, in Washington, the expected burst of fiscal stimulus failed to occur. Despite a supportive rollback of Obama-era regulation, the failed effort to replace the Affordable Care Act and the uncertainty of forward motion on other Trump priorities, such as tax reform and an infrastructure bill, sapped the markets’

confidence in the dollar. By contrast, economic growth prospects brightened in the eurozone, and in Canada, Australia, and China. Britain also experienced growth that belied expectations of a slowdown in the wake of the Brexit vote.

The result was a decline in the value of the dollar at a pace that nearly matched that of the dollar’s impulsive rise in mid-2014.

### Looking ahead

Rapid market moves are often followed by periods of consolidation. Trades made in anticipation of specific developments sometimes require a period of waiting to see if the expectations are played out. The currency market may be looking at such a pause for the near future in response to the rapidity of the last months’ trend.

Going forward, however, the expectation of Wells Fargo Securities’ currency forecasters is for expanded global growth, continued convergence of monetary policies, and a trend decline in the value of the dollar. This in turn would be supportive for the U.S. economy in terms of exports, and might embolden the Fed to continue its campaign to return interest rates to a normal level.

Markets are fickle, however. It always pays to be prepared for a surprise event that might change market perceptions again — and produce yet another about-face. ■

The image shows two men in business attire standing in an office. The man on the right is wearing glasses and holding a tablet. The background features large windows with blinds. A colorful gradient overlay, transitioning from yellow to orange to red, is positioned at the bottom of the image, partially covering the men's lower bodies and the text.

Future *Forward*  
**Innovation**



## The rise of RegTech

### Applying technology to aid in the compliance process

Since the global financial crisis of 2008, the regulatory requirements for banks have expanded significantly. Analysts tallied a 492% increase in the annual volume of regulatory changes between 2008 and 2015.<sup>1</sup> Global banks must now track, interpret, and adhere to an average of 200 individual regulatory changes each day — or nearly 50,000 per year.<sup>2</sup>

Banks today spend a staggering \$80 billion on governance, risk, and compliance, and devote as much as 15% of their workforce to related activities.<sup>3,4</sup> Compliance requirements impact not only how banks interact with their wholesale and retail customers, but also their global correspondent banking relationships. A recent report directly links the high cost of compliance and risk management

(including fines for missed requirements) to a five-year decline in correspondent banking relationships.<sup>5</sup>

The immense cost and effort for banks comes, in large part, from aging systems, manual processes, and a lack of infrastructure to manage the volume of data and analytics now required for compliance.

## RegTech universe



As a result, many financial institutions may not be able to manage their compliance workload in an efficient or automated fashion.

RegTech or “regulatory technology” providers hope to change that.

### **A range of new APIs, artificial intelligence, and cloud services**

RegTech is a new and growing subset of Fintech. These nimble technology companies aim to help banks and other players in the financial services sector automate and streamline the process of regulatory compliance.

Creating a simpler, more efficient process, in turn, reduces the effort of compliance. Banks can benefit from cost savings, improved customer service, and, as one industry expert recently told *The Economist*, potentially take back customers previously deemed unprofitable, due to cost and risk concerns.<sup>6</sup>

Since 2012, RegTech start-ups have raised more than \$2.3 billion to fund their solutions.<sup>7</sup> Industry players are exploring everything from cloud computing and application program interfaces (APIs), to artificial intelligence (AI), data mining, and predictive analytics.

RegTech applications deliver a wide range of functionality that can ease bank operations at various stages. For example, identity management and control solutions support counterparty due diligence and Know Your Customer (KYC) processes. Approximately 3,700 member banks already use the KYC data registry provided by SWIFT<sup>8</sup> to improve data collection with their correspondent bank networks.

Transaction monitoring applications, such as the Sanctions Screening tool launched by SWIFT, provide real-time alerts to improve detection of potentially noncompliant transactions. Automated reporting tames the massive amounts of regulatory and customer data with advanced analytics that can quickly deliver actionable insights. These are just a few of the tools now on the market.

Financial institutions are ready for new solutions. Two-thirds of industry stakeholders cite RegTech as “very important” to managing future regulation and reporting; more than half plan to increase their RegTech investment over the next three years.<sup>9</sup> Bank spending on governance, risk, and compliance is expected to grow to \$120 million over the next five years.<sup>10</sup>

## Which RegTech services are right for your bank?

As your institution grapples with the changing landscape of regulatory compliance, RegTech will likely be a part of your solution set.

Here are some important considerations as you evaluate your options:

- **Which processes are most important to automate and streamline?** Start with a close inspection of your organization's current state and top pain points. Where do manual processes, lack of information, or disparate systems cause bottlenecks or impede your customer service? Where does lack of access to data or reporting create undue risk? Make these areas your priority when seeking RegTech solutions.
- **Where can you pilot artificial intelligence solutions?** AI and machine learning use computer algorithms and models to find patterns in data, then predict the probable outcomes. Processes that require subject matter expertise but are difficult to conduct at scale make good candidates for these services.

- **Where can you leverage APIs and cloud services?** Using subscription services, flexible open platforms, and direct connections to regulatory systems (rather than hosting technology in-house) can dramatically reduce your development time and costs — without sacrificing speed or security.
- **Who will “own” RegTech in the organization?** An internal champion will be critical to success, but leadership might not come from traditional sources. RegTech bridges traditional boundaries between IT, compliance, and risk management departments.

Whichever solutions you choose, implementing RegTech can help your bank increase operational efficiency, reduce the cost of compliance, decrease fraud, and improve the customer experience.

**Learn more:** The newly formed [International RegTech Association \(IRTA\)](#) focuses on the people, tools, and policies required to advance RegTech innovation in the financial services industry. It aims to unify RegTech globally and create a collaborative ecosystem. ■

1. Thomson Reuters research, as cited in Deloitte, “The RegTech universe on the rise,” 2017
2. Boston Consulting Group, “Global Risk Survey 2017: Staying the Course in Banking,” March 2017
3. Let's Talk Payments, “How Can RegTechs Help the Financial Services Industry Overcome the Burden of Compliance?,” May 9, 2016
4. Deloitte, “The RegTech universe on the rise,” 2017
5. Financial Stability Board, “FSB Correspondent Banking Data Report,” July 4, 2017
6. The Economist, “A crackdown on financial crime means global banks are derisking,” July 8, 2017
7. CB Insights, “RegTech Market Map: The Startups Helping Businesses Mitigate Risk and Monitor Compliance Across Industries,” February 6, 2017
8. SWIFT KYC data registry
9. Banking Technology & BearingPoint, “How RegTech savvy are you?,” RegTech survey, June 5, 2017
10. CB Insights, “RegTech Market Map: The Startups Helping Businesses Mitigate Risk and Monitor Compliance Across Industries,” February 6, 2017

A photograph of three business professionals in a meeting. A woman with blonde hair, wearing a blue blazer, is seated in the center, looking towards a man on the right who is wearing a maroon sweater. A man on the left, wearing a dark sweater, is seen from the back, looking at the woman. They are sitting at a table with a laptop and a glass. The background is a large window with a view of a modern building. The text 'Future *Forward* Innovation' is overlaid on the image in white, with 'Future' and 'Innovation' in a bold sans-serif font and 'Forward' in an italicized sans-serif font.

Future *Forward*  
Innovation



## Banks embracing APIs to improve — and expand — their customer relationships

Two-way information sharing will deliver the greatest value

With more of our personal and professional lives now linked to the digital world, global banks have a new opportunity to deliver value to their customers — value that goes far beyond simply facilitating a payment transaction. Application programming interfaces, or APIs, are helping banks evolve their customer relationships through faster, easier access to data and seamless, embedded delivery of services.

APIs allow banks to embed predeveloped capabilities into any part of their digital environment: A website, customer portal, mobile app, or back-office system. The result is efficient, machine-to-machine communication that occurs in real time, and without the limitations of batch processing.

### **APIs offer endless possibilities**

The pressing question for banks is no longer “when” to launch APIs. For savvy global banks, the question is *which* APIs, and in collaboration with what outside providers?

Whether we realize it or not, APIs are all around us. They facilitate everything from

*“We forecast that real GDP growth in China will slow somewhat in 2018 relative to the rate that likely will be achieved this year.”*

allowing a ridesharing service to identify your location to helping you book a table at your favorite restaurant to enabling you to verify that your shoe size is in stock before you visit the store. Tech developers across industries have relied on APIs for years to launch new capabilities faster and reduce development costs. Instead of building functionality from scratch, they leverage the work of experts in the field.

Within financial services, PayPal represents one of the first API success stories. Founded in 1998, the payments innovator has built a thriving business with APIs that make it fast and simple for merchants to accept electronic payments. Recently, Fintech companies have capitalized on the API revolution and brought these proven technical capabilities into the mainstream. Fintech APIs now power mobile wallets, consumer lending platforms, live FX rates — and more.

Regulatory changes are also fueling broader adoption of APIs. Europe’s Payment Services Directive (PSD2), for example, mandates that banks must open up data access to third-party providers in 2018.

## **Collaboration benefits banks and Fintechs**

Done right, APIs can offer more opportunities for customers to engage with their bank. However, banks must think beyond simply opening up access to third parties who want to integrate bank account balances and other data into their solutions.

Banks must consider where featuring Fintech capabilities or APIs from other industries can create new connections or efficiencies for banking customers. For example, would bank customers value real-time access to their credit score while within a bank application or work flow? From a bank-to-bank perspective, financial institutions can leverage APIs and Fintech innovations to validate account number, currency of account, and name before making a payment on behalf of their customers, or, in the case of a potential fraudulent activity, determine the location of the party initiating the payment. These are the types of opportunities that APIs make possible.

While a collaboration between traditional financial services organizations and Fintechs may sound strange, the relationship offers benefits for both sides. Banks deliver an established customer base, robust transaction security, and regulatory expertise, but often struggle to move quickly and nimbly with new technologies. Fintechs, with more agile cultures and singular focus, can bridge this gap.

Wells Fargo launched an API developer portal, the Wells Fargo Gateway, in 2016.

The site makes it easy for banks, Fintechs, and other providers to integrate best-of-breed digital capabilities. Current APIs support location services, validation of account ownership, real-time payments, FX origination, and more.

The future of banking means making it faster, easier, and simpler for wholesale and retail customers to accomplish their financial goals. With this view in mind, the possibilities for the financial services industry are nearly endless. ■

© 2017 Wells Fargo Bank, N.A. All rights reserved. Member FDIC.



A photograph of two men in business suits standing on a rooftop or balcony at sunset. The man on the left is smiling and looking towards the man on the right. The man on the right is holding a briefcase and looking back at the first man. The background shows a cityscape with buildings and a body of water, all bathed in the warm, golden light of the setting sun. A decorative horizontal bar with a gradient from yellow to red is positioned behind the text.

Future *Forward*  
Partnerships



## Partnering to protect the client experience

Working together as a community to prevent fraud and cyberattacks

While the global payments industry embraces innovation and moves toward digitalization and Faster Payments, cybercriminals are becoming more sophisticated, using advanced techniques and social engineering to steal data and funds from clients.

According to the 2017 Association of Financial Professionals Payment and Fraud Control Survey, 74% of organizations were victims of payments fraud in 2016.<sup>1</sup> Cyberfraud threats include online account takeover, where fraudsters gain unauthorized access to customers' computers and conduct unauthorized transactions. Imposter fraud, also known as business email compromise, is where a fraudster poses as a person the customer trusts and tricks the client to send a payment to an unintended recipient.

Email continues to be the preferred operating method for fraudsters. Recent studies show that one in 131 emails are malicious, the highest rate in five years.<sup>2</sup> The FBI reports \$5.3 billion in exposed losses globally due to email compromises through December 2016. Email scams have been reported in all 50 U.S. states and in 131 countries,<sup>3</sup> and is a true global epidemic.

Banks around the world are responding to the threat by making substantial investments to upgrade operating infrastructures to improve detection and prevention of fraudulent transactions. “While the infrastructure investment is critical,” says **Chuck Kohler**, Head of Wells Fargo GPS Sales, “this effort needs to be supplemented by a comprehensive end-to-end payment fraud prevention program designed to protect clients and react quickly when a fraud occurs.”

### Building client awareness

Educating clients regarding fraud prevention and detection is the first step in the battle against fraud. Wells Fargo has launched an extensive education program globally. We strongly believe banks must continually educate staff and clients regarding best practices to prevent fraud. These practices include:

- Authenticating all change requests and watching for red flags
- Verifying electronic or unusual requests through a channel other than through which it was originally received
- Using official contact information on file to verify requests; never using contact information provided in the request
- Never giving out online banking credentials
- Monitoring accounts daily and using notification and alert services
- Being wary of token prompts that appear to be a sign-on
- Disregarding on-screen messages requiring immediate action

- Never clicking links, opening attachments, or installing programs from unknown senders
- Updating antivirus programs regularly
- Implementing dual custody for electronic payment initiation and ensuring both users are on different devices
- Authenticating requests before processing a payment and paying close attention to payment details
- Generating transactions from a stand-alone PC with email and web browsing disabled
- Never accepting or allowing changes to bank account information via email

Keeping up to date is vital. For the most recent information regarding operating best practices and fraud prevention, please visit [Wells Fargo's Treasury Insights](#) fraud protection page.



*It is a core responsibility of all participants in the global payments community to maintain a safe and secure operating environment.*

### **Protecting the integrity of the global payments system**

Properly authenticated payment instructions received from clients via e-banking and mobile channels are expected to be processed on a timely basis and in a secure manner. It is a core responsibility of all participants in the global payments community to maintain a safe and secure operating environment. Protecting and preventing fraud requires a properly trained and responsive staff, coupled with robust operating processes supported by best-in-class technology.

In addition to segregation of duties and regular access/entitlement reviews, operating system architecture and procedures should include:

- Limiting system access to include only required personnel
- Establishing appropriate transaction approval limits and velocity controls
- Protecting user access credentials
- Ring-fencing networks used for critical business operations from the open Internet

- Keeping operating systems up to date with appropriate antivirus and firewall applications
- Deploying detection capabilities for abnormal events, such as failed log-ins or sequential log-ins from different devices under the same user name
- Ensuring that third-party service providers (vendors and service bureaus, for example) have secure and robust cybersecurity programs and controls in place

Securing the financial messaging infrastructure is vital to the global payments industry. At Wells Fargo, we fully support industry initiatives, including the SWIFT Customer Security Program (CSP) and encourage:

- Installing SWIFT-standards releases at the earliest opportunity
- Reviewing Relationship Management Applications (RMAs) on a regular basis and eliminating dormant relationships
- Implementing RMA plus to gain additional control of message types
- Linking the RMA to customer due diligence and security practices
- Implementing the appropriate risk-based traffic pattern procedures and removing inactive RMAs

If making a link, say: “Learn more about the SWIFT CSP [here](#).”



## Detection and prevention

Alert, experienced staff who have been trained to recognize warning signs, behavioral, and/or pattern changes remain one of the most important safeguards against fraudsters. Operational best practices include:

- Requiring complete transaction details (for example, full sender and beneficiary address details)
- Establishing real-time balance and/or transactional alerts (by day, time, and/or amount)
- Prompting account reconciliation

Around the world, real-time transaction monitoring capabilities are being enhanced by financial institutions. Using Artificial

Intelligence (AI) to create a behavioral map of client transactional activity is widely used within the card business. Within the U.S. domestic ACH system, name and account number matching has been successfully implemented, though no equivalent exists yet for cross-border payments. Corporate cash management applications identify beneficiary name and account number changes, which may be indicative of heightened transactional risk. Profiling incoming credit activity for incoming funds to an account is being considered by many institutions.

SWIFT has recently introduced Daily Validation Reporting to assist financial institutions in detecting unusual payments. Although post-transaction, the reporting feature highlights large or unusual transactions during the day and assists in the detection and response to unauthorized transactions. Transaction banks and SWIFT are creating data warehouses and evaluating real-time detection tools.

## Moving to a global operating model

“Speed, cooperation, and coordination are essential when attempting to recover funds sent to an unintended beneficiary,” says **Chris Jenkins**, Head of Client Experience for Wells Fargo Global Payment Services. “More and more institutions are establishing fraud response teams, with defined roles and responsibilities, to establish clear rules of engagement and to respond quickly and consistently. Operating playbooks are being developed to investigate, escalate, and report to the appropriate authorities.”

Multiple industry efforts are under way to build a global operating standard. The Payment Market Practice Group is developing standards to expedite cancellation and recall of funds that were originated in error or were fraudulent in nature. Enhancements to SWIFT gpi are being developed to support a real-time cancellation process that leverages the unique transaction identification number that each transaction will carry. There are efforts beginning with the Bankers Association of Finance and Trade (BAFT) to standardize a Letter of Indemnity structure globally. While there are still significant legal and operational challenges to overcome, these efforts represent significant enhancement over today's operating environment and are moves to a global operating standard which will improve the industry's response time.

When a fraud occurs, timely reporting of problems and security incidents to industry and regulatory bodies, as appropriate, should always be encouraged. Cooperation between Fraud, Cybersecurity Intelligence, and Compliance Risk Management teams in managing unusual transactional activity and remediation actions is critical to respond to any cyberattack.

Only by working together as a community can we protect our customers and the client experience. ■



1. 2017 Payments Fraud and Control Survey, Association of Financial Professionals, page 2.

2. Symantec Internet Security Threat Report April 2017, page 8.

3. Business E-Mail Compromise Email Account Compromise The 5 Billion Dollar Scam FBI public service announcement May 4, 2017, Alert Number I-050417-PSA. <https://www.ic3.gov/media/2017/170504.aspx>

Together we'll go far



© 2017 Wells Fargo Bank, N.A. All rights reserved. Member FDIC.

Wells Fargo & Company conducts business outside the U.S. through various companies, including duly authorized and regulated subsidiaries and affiliates in Asia, Canada, Europe, and Latin America. All products and services may not be available in all countries. Each situation needs to be evaluated individually and is subject to local regulatory requirements. Member FDIC. Deposits held in non-U.S. branches are not FDIC insured. IHA-4581002