A FINEXTRA WHITE PAPER

PRODUCED IN ASSOCIATION WITH BOTTOMLINE TECHNOLOGIES

JANUARY 2016

THE NEED FOR COMPLIANCE AND CONTROL IN A CHANGING LANDSCAPE:

Technology, process and business strategies to turn compliance into competitive advantage

Bottomline Technologies | Finextra

CONTENTS

01
EXECUTIVE SUMMARY

It is well-recognised that a number of factors are dramatically changing the regulatory landscape for banks and financial institutions. These include the post-financial crisis focus on improving the safety and resilience of the financial markets, efforts to stimulate competition in financial services while protecting consumers, and an increased drive to fight financial crime.

While much of the new regulation is not specifically aimed at corporates, the fact that banks are being mandated to change their structures, processes and behaviours certainly creates a knock-on effect for corporates – sometimes positive, sometimes negative. Corporates must understand the impact of banking regulatory change and implement a strategy in order to minimise any downside and maximise any upside.

In a similar vein, some corporates are starting to put in place capabilities to comply with regulations that currently target banks – such as in the area of anti-money laundering and sanction filtering – for peace of mind and in anticipation of these rules being extended to apply to corporates as well as banks.

The recent wave of new regulation comes on top of an existing framework of controls implemented since the turn of the millennium, which have required corporates to put in place ever-more robust internal controls and transparent financial accounting and reporting processes. An increasing incidence of internal and external fraud – exacerbated by the growing cyber-threat – also demands constant vigilance and ongoing improvements in protection regarding processes and technology. As well as investing to protect themselves from cyber-threats, corporates need to keep up with the improvements to security that their banks and other financial institutions are making. There is a knock-on impact for corporates, which must adapt to ensure the same exacting levels of security along the transaction chain.

At the same time, corporates are impacted by a number of industry and regulatory-driven initiatives to improve efficiency in payments and in the financial supply chain. This requires standardisation and automation to avoid penalties and to ensure they benefit from the cost and risk reduction that operational efficiency brings to a business.

There are two other important factors to consider. One is the volume of regulation with which corporates need to cope. To give some context, the EU has issued in the region of 30 new rules impacting the financial markets since 2008. And there were reportedly some 40,000 compliance updates imposed globally in 2014. Appendix A lists just some of the significant pieces of regulation that have been implemented since 2002.

The other factor is the challenge of managing change. The environment is not static, and there is a constant requirement to update processes and technology in order to comply with regulation and to tackle the risks generated by inefficiency. Corporates need strategies to enable them to gain, and maintain, control in a continually changing landscape.

Overall, today corporates are facing a greater challenge from compliance in its broadest sense than ever before. The purpose of this white paper is therefore to explore the compliance challenges impacting corporates, and the technology, process and business responses which they can formulate in order to comply, while also generating operational and commercial benefits.

02

COMPLIANCE CHALLENGE 1: FRAUD, CYBER AND FINANCIAL CRIME

KEY FACTS

- **Insider fraud is increasing:** KPMG data shows £262m losses in UK due to white collar crime in H1 2015
- **The cyber-threat is growing exponentially:** the estimated annual cost of global cyber-crime is $100 billion
- **The regulatory environment is getting tougher:** there are new data protection rules on the horizon, the 4th Anti-Money Laundering Directive is biting, and financial sanctions are increasingly being imposed as part of countries' foreign policies.
- **Corporates must beef up internal and external controls** to fight fraud, cyber and financial crime threats

Corporates are well used to documenting and implementing internal controls to comply with Sarbanes-Oxley (and other national equivalents), imposed in the wake of major accounting scandals in the early part of this century. They are also complying with data protection laws and the implications these have on data storage and document management.

Despite all the protections in place, levels of **internal fraud** are increasing. KPMG's Fraud Barometer for the UK shows that during the first part of 2015 'white collar crime' had surged, as those in positions of responsibility or management have abused their power to commit frauds totalling £262m. The KPMG study for 2014 also revealed a significant increase in insider fraud – with the number of employee perpetrated frauds in the £1-10m range growing more than tenfold. Meanwhile a study conducted by the Association of Certified Fraud Examiners in the US showed fraud losses against privately-held organisations accounted for the loss of 5% of all revenues annually. And one study suggests 59% of employees admit to having stolen company data when leaving previous jobs.

External fraud is also on the increase. In 2014, almost 277,000 frauds were reported by more than 245 organisations to the National Fraud Database of not-for-profit organisation Cifas. This equates to 758 frauds a day, or 31 per hour. As regards corporates, the KPMG data for 2014 showed that whereas previously financial institutions and government bodies had been the biggest victims of fraud, commercial businesses were becoming more of a target. The number of cases of companies being scammed increased from 64 to 107, at a value of £98m (versus £76m in 2013).

Regulatory pressure is having an impact on reported fraud cases as well. Financial services firms were liable for more than half the value of all reported fraud in the UK between 2012 and 2013. BDO noted that the ever-increasing regulatory and compliance burden imposed on financial services firms means that fraud which historically may not have been reported, but rather dealt with privately in-house, is now coming out, driven by a growing demand for transparency.

Much of the fraud – internal and external – being perpetrated against corporates is low-tech and not very sophisticated (like invoice fraud for example), though it is no less effective. In 2015 a former BMW-Mini worker was jailed in the UK having been convicted of siphoning off almost £6m from the car manufacturer by altering supplier payment details on invoices in his favour.

Of course, highly sophisticated **cyber-crime** grabs many of the headlines, fuelled by high-profile hacks like the recent TalkTalk attack. The estimated annual cost of global cyber-crime is $100 billion – equating to 556m victims per year, 18 per second. The response is an increasing investment in sophisticated security measures to combat the cyber attackers. By 2017, the global cyber-security market is predicted to amount to $120.1 billion, compared to $63 billion in 2011.

One entity which is responding to the threat of cyber-crime is Bacs in the UK, which is beefing up its security protocols, requiring its users to deploy TLS and SHA-2 protocols to protect their Bacs communications with VocaLink from mid-2016. This is just one concrete example of a mandate for corporates to invest in improved **security** technology. They must achieve compliance quickly in order to maintain business continuity at the point of switchover in June 2016 and failure to do so will prevent them from being able to submit via Bacs. In addition to achieving compliance with this specific requirement, implementing a policy of multi-factor authentication enforces a more secure access and approval environment, to reduce the risk of fraud.

JOINING THE FIGHT AGAINST FINANCIAL CRIME

There is an increased emphasis on fighting financial crime, including but not limited to that perpetrated by cyber-criminals, and covering **KYC, AML and compliance with economic sanctions**. While financial institutions are clearly at the forefront of the fight and are the primary focus of regulations in this area, corporates also need at the very least to be aware of the various regulations.

Increasingly, and depending on the degree to which they do business across borders, corporates may need to implement increased controls, not only to remain compliant but also to be able to provide audit trail information about suspicious beneficiaries, payments and transactions flagged by their banks. If a corporate is able to screen a transaction against a sanctions list before submitting it to a bank, the corporate has additional peace of mind and avoids the reputational risk of being identified by its bank as having proposed payments to black-listed organisations or individuals. In addition, similar **screening solutions** can be deployed to identify inappropriate payments being directed to employees, thus helping to prevent internal fraud issues.

In the fight against fraud, it is hugely valuable for a business to be able to track its employees' use of mission critical applications, to identify any anomalies and suspicious behaviour. This non-intrusive way of monitoring user activity enables a corporate to capture and replay such behaviour, rather like a CCTV, not only recording any information, such as account numbers, which have been changed, but also which screens have been viewed. Having such systems in place offers an early warning of inappropriate behaviour by employees and also acts as a strong deterrent to anyone thinking of committing a fraud. In the worst case scenario, this recorded activity can also be used as evidence in legal proceedings, reducing the likelihood of further fraud.

RECOMMENDED RESPONSES

- Increase internal controls, further exploit software with rules embedded to ensure adherence to processes, control of entitlements for access and approvals, as well as data protection
- Increase security technology investment – including TLS/SHA-2 for Bacs payments
- Explore automated KYC/AML/Sanction Screening solutions
- Consider how trusted partners can help

VOICE OF THE CORPORATE

The TalkTalk cyber-attack has pushed security even higher up the agenda for many corporates. As Sean Earlam, UK&I Senior IT Manager at Hays Recruitment says, the imperative for any business handling customer data is to prevent data breaches. “We cannot afford our data to be hacked,” he says. “Hays is in the business of recruiting temporary and permanent workers, and we cannot allow the database of information associated with our clients and candidates to become available on the wider internet. The reputational threat to our business of data breaches is as much of a worry to us as are financial losses.”

Security has always been a focus for Hays, and the company is now redoubling its efforts in response to the growing cyber-threat, Earlam continues. The security project currently under way at Hays involves phasing out older machines, enhancing security around its key systems and leveraging the most up to date security capabilities of its providers and its internal security policies and procedures. Hays has committed significant time and money to the security programme, which it is running alongside its existing IT projects, Earlam confirms.

Hays’ UK data centres are managed by a third party, and the new security policy enforces the maintenance and use of administration passwords only by authorised users, Earlam explains. Security around its front office database containing client and candidate information has been increased, and around its back office ERP system additional encryption has been added and a security access policy at a roles and responsibilities level implemented. Hays will be using cloud-based solutions for payments and cash management from Bottomline Technologies. “The Bottomline solutions integrate with our ERP system and we are busy upgrading to the latest version of our payment product to take advantage of its inherent enhanced security, including TLS/SHA-2 for our Bacs payments,” Earlam says.

“The aim is that no cyber-criminal could get access to our data in the first place,” Earlam says, “and in the very unlikely event that they could, all the sensitive information is encrypted so would be worthless to a hacker. The whole driver behind our programme is to ensure our data is safe. We are relying on the highest levels of security from our technology providers, as well as reviewing and improving our own internal controls.”

Hays’ current project bolsters an already strong focus on security. “Our existing fraud protection activities are part of our ‘business as usual’,” Earlam confirms. “Much of this is provided by Bottomline Technologies. I have the information I need to detect any ‘foreign’ activity that takes place internally. All our email servers are monitored at the user level and we have the ability to detect any untoward activity immediately. What we have in place is robust enough to provide us with the detection we need at all the right levels.”

Hays also looks to Bottomline to help it meet its other compliance obligations, he adds. “There is a requirement on us to remain in compliance with SEPA, ISO and e-invoicing standards, and we look to Bottomline to help us meet these compliance obligations at all times,” Earlam concludes.

03

COMPLIANCE CHALLENGE 2: REGULATION IMPACTING BANKS

KEY FACTS

- **Basel III**
  - **Minimum capital requirements**: all banks must hold 7% of risk weighted assets in common equity or core tier one capital; regulators, such as the Bank of England, will require higher capital ratios on systemically important banks, as well as counter cyclical buffers to protect the financial industry against future losses.
  - **Maximum leverage ratios**: banks are restricted to a leverage of 33 times their core tier one capital; leverage will be calculated without any risk weightings being applied and all exposures – including off-balance sheet items – will be included in the assessment.
  - **Liquidity ratios**: a liquidity coverage ratio requires banks to hold enough high-quality liquidity assets to cover any net cash outflows over a period of 30 days; a net stable funding ratio will require banks to hold sufficient assets with a residual maturity of one year or more to finance longer term, illiquid assets.
  - **Corporates** may find banking services, including lending and deposit products, will be changed or withdrawn; where services are still provided, pricing or remuneration may change.

- **PSD2**
  - **Opens up the EU payment market** for new regulated entities offering consumer or business payment services based on access to bank accounts – known as Third Party Providers of Payment Initiation Services and Account Information Services
  - **Introduces strict security requirements** for initiating and processing electronic payments and protecting consumers' financial data
  - **Enhances consumers' rights**, for example reducing the liability for non-authorised payments
  - **Prohibits surcharging** on cards whether the payment instrument is used in shops or online
  - **Corporates** may see opportunities to become regulated as new Third Party Providers and/or be able to benefit from the services of these new Third Party Providers

Post-financial crisis regulation, along with new rules to improve consumer protection and encourage greater competition in financial services, are reshaping the regulatory landscape for banks. In turn, these regulations have impacts on corporates – some direct, some indirect. At the very least, corporates need to understand what the regulations mean for their banks and consequently for them. In some cases corporates may need to invest in new solutions to meet their needs, and in others they may need to decide whether to invest in new capabilities to capitalise on the opportunities created by regulation impacting the banking industry.

One example of regulation targeting banks which will impact corporates is **Basel III** (see box). In this case, corporates are likely to see a reduction in the effectiveness of their banking relationships in key areas. Banks are likely to require longer-term deposits to help them meet their obligations under Basel III, and will reduce the remuneration on short term deposits not considered as "operational" since they are now regarded as flighty. Banks are also raising the cost of borrowing and continuing to reduce their overseas branch networks. While corporates are globalising, banks are doing the opposite – which means that having had a goal of reducing the number of banking relationships they maintain globally for several years, corporates are now likely to have to increase that number again to ensure global reach. Corporates really need improved cash forecasting and better sweeping facilities in order to minimise borrowing and maximise return on any surplus cash, but notional pooling will be harder for banks to provide, as there are now greater restrictions on banks wanting to net-off assets and liabilities across entities.

As a consequence, corporates will need to source bank-independent arrangements for **sweeping and pooling**, along with technology solutions to help them **manage multiple bank relationships** globally.

Another example of banking industry regulation with an impact on corporates is **PSD2** (see box). Designed to increase consumer protection and to stimulate greater competition in the financial services industry, PSD2 creates a number of opportunities for corporates. Some – for example retailers – may decide to **become regulated** under PSD2 as Payment Initiation Service Providers or Account Information Service Providers, opening up a new line of business providing their customers with a seamless payment service as part of the overall buying experience.

Other corporates are more likely to benefit through having a **greater choice of payment services** from existing providers and new entrants into the industry. Under PSD2 banks are obliged to develop APIs to open up access to bank account information to a new breed of Third Party Providers which will provide **aggregation services**, bringing together bank account information from multiple sources. This will address a key pain point for multi-banked corporates. Getting a clear picture of cash and risk positions across multiple accounts is expensive, especially for smaller businesses, and this could be a clear benefit of PSD2 for corporates. Some of the more advanced corporates are already achieving visibility across multiple banks by using a SWIFT service bureau to access balance and transaction reporting and to manage payment flows securely.

RECOMMENDED RESPONSES

- Understand commercial opportunities created by new regulation
- Understand commercial challenges created by new regulation
- Work with banks to understand the impact of change
- Plan and execute technology and business strategies to optimise change, considering trusted partners where relevant

VOICE OF THE CORPORATE

"Treasury might not be glamorous, but it's crucial to any enterprise, and needs sustainable banking relationships. That sustainability is now under threat from the triple forces of politics, technology and regulation, while Basel III – which is already having an impact – will get much worse."

DANIEL BLUMEN, PARTNER, TREASURY ALLIANCE GROUP

"Banks are dealing with a swathe of regulations that aren't very clear and it is hurting the customer experience."

DAMIAN GLENDENNING, TREASURER, LENOVO

04

COMPLIANCE CHALLENGE 3: CORPORATE REGULATIONS AFFECTING OPERATIONAL EFFICIENCY IN PAYMENTS AND FINANCIAL SUPPLY CHAIN

KEY FACTS

- **The SEPA journey continues**
  - **The most recent SEPA deadline on 1 February 2016** may require further action from corporates: they must indicate the IBAN, the BIC is no longer required, they must use the SEPA ISO 20022 XML format and "niche schemes" need to be SEPA compliant or phased out
  - **For euro bank accounts not held in the Eurozone** SEPA deadlines are due to be enforced in October 2016 – impacting UK corporates and other non-Eurozone countries
  - **Beyond compliance, there are opportunities for corporates to gain further efficiencies**: review bank account structures, streamline banking partners within Europe, and optimise internal treasury structures
  - **The cost of further technical changes can be offset** by working with cloud suppliers

Operational efficiency in payments and the financial supply chain is an ongoing strategic objective for many corporates. In Europe a driver for this is the European Commission's Digital Agenda and continued focus on creating an efficient single market. Cost and risk reduction are also major commercial drivers. Underpinning these initiatives is the adoption of and adherence to international standards to streamline communication between entities in the transaction and supply chains. **ISO 20022** is now the most well-known and best-established of these and corporates are most feeling the impact of the move to ISO 20022 in the area of **SEPA**.

The first SEPA deadlines hit in 2014, and a new set of requirements must be met by February and October 2016 (see box). As always, depending on the level of SEPA impact on a corporate and by its appetite for investment in making the changes, there is likely to be some eleventh hour compliance activity. One valid option is to further leverage **data conversion and validation services** from trusted fintech and cloud suppliers. If the costs and time involved in making changes to ERP systems are prohibitive, corporates can leverage middleware solutions to insulate themselves from the changes, and continue to focus on their core business activities.

Beyond compliance, there are opportunities to drive further efficiencies off the back of SEPA (see box). Corporates can consider – again with partners where relevant – creating **payment factories** to benefit from centralisation and scale in their payments activities. SEPA is the ideal starting point for a payment factory project. Corporates that are SEPA compliant will have already achieved standardisation of euro payment and Direct Debit instruments across the Eurozone. They will be starting to feel the benefits of standardised and centralised internal processes, as well as achieving lower processing costs and reducing their number of bank accounts in the Eurozone. They should also be benefiting from lower bank fees on compliant bulk payments and Direct Debits, and experiencing lower operational risk, easier audit processes and improved cash flow forecasting and reconciliation.

So now the opportunity is to go beyond the Eurozone and SEPA, to achieve similar benefits in other currencies and geographies, with a payment factory – which can sit in the secure cloud – acting as the core platform for streamlining multi-country payment and collection arrangements, whether regional or global.

A payment factory requires a single, centralised platform for all domestic, regional and global payment types – treasury, payroll and expenses, Direct Debits, supplier payments and cheques. While efforts are under way globally to eliminate paper cheques these initiatives are arguably coming years too late for corporates. For certain geographies, such as North America, France and Ireland, corporates still need to process cheques, and many have taken advantage of **outsourced cheque services** to streamline multi-currency cheque production and distribution, as part of their payment factory projects – demonstrating that payments factories can be used not only for electronic payments but also to efficiently manage the tail-end of paper payment instruments.

The main benefits of a payment factory are centred around cost reduction, operational risk mitigation and standardisation. A payment factory becomes a centre of excellence for payments. It has secure, standardised interfaces and standardised processes, with strong data conversion capabilities to increase straight through processing. It provides centralised controls, with secure but

configurable segregation of duties: central treasury can achieve pan-enterprise visibility, whereas local units can review regional activity and bank accounts. Full audit trail functionality supports compliance. While payment factories must have the flexibility to work with local protocols for communication with banks, they are also highly suited to standardising bank connectivity – for which large corporates are increasingly adopting SWIFT.

It is important for cloud-based payment factories to have secure multi-bank connectivity. It is therefore an advantage for corporates to select a technology partner which not only offers cloud-based payments solutions but is also a SWIFT service bureau, with expertise in connecting securely with a wide range of banks internationally. There is a small number of super bureaux which are offering a growing range of protocols and connectivity options, such as Host to Host solutions and EBICS, the latter of which is widely used for secure corporate to bank communication in Germany, France, Benelux and Switzerland. This is cheaper than using SWIFT in these countries, which means a super bureaux can structure a solution that best suits a customer's needs, according to its geographical footprint. An example of this lowest cost routing in the UK is of course Bacs, which is a unique scheme offering Direct Corporate Access to VocaLink for clearing and settlement of Sterling payments. There is a growing market trend for corporates operating in the UK to adopt Direct Corporate Access for Faster Payments, for which the number of sponsor banks is set to increase. By combining a SWIFT bureau with outsourced Bacs and Faster Payments capabilities, a cloud payments solution provider is ideally positioned to offer its customers an optimal platform for efficient payments and cash management, spanning multiple payment types, protocols, connectivity options and messaging networks.

Supporting this and creating a further opportunity for corporates to leverage the benefits of standardisation on ISO 20022 is the **Common Global Implementation Market Practice** (CGI-MP) initiative, which is aiming to simplify implementation of ISO 20022 for corporate users and thereby promote wider acceptance of the standard. The goal is that a corporate can use the same message structure for all their payments and collections with all of their transaction banks and reaching any payment system across the globe. Again, there is an opportunity for corporates to leverage their service providers' engagement and involvement with CGI-MP and ISO 20022 to further exploit the advantages of international standards.

GENERATING EFFICIENCIES IN THE FINANCIAL SUPPLY CHAIN

KEY FACTS

- **A number of initiatives require corporates to improve efficiency of invoicing processes**
  - EU Directive requires e-invoicing for government procurement (though some states have been more proactive than others)
  - Work continues on a European e-invoicing standard which will likely wrap XML in PDFs/a document(s) – but progress is slow
  - The EU Directive on Combating Late Payment in Commercial Transactions is already in force, mandating maximum payment terms and sanctioning significant penalties which at least in theory give SMEs some teeth in the face of late payment
  - Outsourcing to a trusted cloud provider is a way to achieve efficiency in the financial supply chain today – especially if the supplier also offers payments factory capabilities in the cloud – to support compliance with regulation, and to be in a good position to exploit any new e-invoicing initiatives/standards

At an industry level there is also a growing focus on making financial supply chains more efficient, and a number of regulations and industry initiatives in this area are impacting corporates.

E-invoicing – and standards for e-invoicing – have been the focus of EU Directives for some time, with the Commission's view being that SEPA is the ideal platform from which to launch a European e-invoicing initiative and generate estimated savings of more than EUR60 billion per year. Some EU states have been more proactive than others in mandating the use of e-invoicing in government procurement processes (the UK has not been at the forefront here) but overall the take-up of e-invoicing has been slower than expected.

Some progress is being made. According to a recent report from Billentis, some 42 billion bills and invoices were likely to be sent and archived paper-free in 2015. But the burden of paper invoicing is still heavy. Labour-intensive, error prone and costly, paper invoicing requires manual intervention, causes slow invoice reconciliation and friction between suppliers and buyers, and can lead to poor cashflow management.

E-invoicing enables businesses to remove manual processes, speed up invoicing cycles and eliminate non-value add activities – significantly reducing costs. However, adoption is being held up by a number of factors. One is confusion about legal status. Another is the need to maintain parallel paper and electronic processes because not all businesses move to e-invoicing at the same pace.

A major stumbling block has been complexity and fragmentation in the market and the lack of a standard format for e-invoicing and of interoperability between e-invoicing systems. Originally the Commission set out a standard which – to cover the invoicing needs of so many industries – became so large as to be unmanageable, and required simplification. There is currently a global e-invoicing project under way - UN/CEFACT CII - which is being fed into by eBes, and is aiming to achieve this. It is driving a standard called CEN MUG, likely to be based on a proven format, either ZUGFeRD, a standard being adopted in Germany, or UBL, a long-established standard. What seems clear is that the eventual standard will be based on wrapping XML in PDF/a document(s) – but it may be a long time coming.

By contrast, there is regulation in place already which requires corporates to increase invoicing efficiency – the **EU Directive on Combating Late Payment in Commercial Transactions.** This specifies that 'member states should promote systems that give legal certainty as regards the exact date of receipt of invoices by the debtors, including a field where the receipt of invoices could generate electronic evidence'.

The Directive and the member state regulations which enact it (in the UK, The Late Payment of Commercial Debt Regulations 2013) specify maximum commercial payment terms as 30 days from receipt of invoice for public sector payers and 60 days from receipt of invoice for private sector payers. If the terms are not respected, creditors are in theory able to charge penalty interest of base rate+8%. Whether in practice they would risk a valued business relationship by charging such punitive rates is open to debate but in theory this regulation gives SMEs considerably more power in the financial supply chain, and the UK government is certainly promoting adherence to the regulation through initiatives such as the **Prompt Payment Code.**

There are clear advantages in streamlining invoicing processes, both to meet regulatory demands already in place, and to be ready to align with e-invoicing initiatives as they become more uniform and widespread. The option of outsourcing the total invoice management process to a provider of managed services in the cloud – able to receive paper or digital invoices and convert both into an electronic format for storage and access, as well as well as send out customer-formatted invoices that can be tracked – is worth consideration. This approach enables a corporate to immediately benefit from e-invoicing while providing a gradual transition to electronic invoicing for its buyers and suppliers.

The trusted partner will also handle adoption of any definitive e-invoicing standard that emerges, and corporates taking advantage of such services are already driving the efficiencies needed in their financial supply chain to enable them to adhere to relevant regulation around late payments.

It is not only to achieve compliance with regulations such as the Late Payment of Commercial Debt Regulations that it is important for corporates to have an efficient invoice approval process. Every business wants to ensure a robust supply chain, especially in an environment where it is regularly reported that SME suppliers are struggling to access credit. A corporate with an efficient payables process, which delivers visibility and control, will greatly benefit from approving invoices in a timely manner, since this opens up strategic opportunities to put these approved payables to good use in improving the business' finances. For example, a cash rich corporate may want to pay early if it can obtain discounts, as part of a dynamic discounting programme implemented by the buyer, or capturing early payment discounts offered by suppliers. This is best practice in cash management, as these discounts effectively reduce the cost of goods or services purchased and enhance margins.

Another scenario in which a corporate benefits from approving its invoices quickly and efficiently is as part of a supplier finance programme. In this situation, approved payables files are passed to a bank which then makes early payment to suppliers by discounting the payables. Meanwhile, the corporate's AP department pays the invoices' full value to the bank at the maturity of those invoices. The optimal situation here for corporates with high credit ratings is that their procurement and treasury teams negotiate with the suppliers which have a lower credit rating so that maturity dates on invoices will be lengthened by say 15 days, in return for which the suppliers will be paid early by the supplier finance banks at an attractive rate of interest. The advantage for the corporate is that they pay the invoices to the bank 15 days later than historically at no extra cost, while their suppliers obtain early payment at a finance rate which is lower than the pricing they would normally be able to access from their own lenders. Many treasurers who are tasked with improving working capital management are beginning to implement the techniques described above to drive efficiency, thanks to faster invoice approval and smarter use of technology.

Furthermore, if corporates choose a trusted partner able to offer both payments factory and invoice management solutions together, they stand to benefit even further from efficiency gains, better working capital management and improved visibility and controls.

RECOMMENDED RESPONSES

- Understand the next set of requirements for SEPA, and consider options for compliance, leveraging partners where relevant
- Determine the options to drive further efficiency from SEPA, formulate and execute strategies to capitalise on these
- Look at the potential of ISO 20022 and CGI-MP to generate additional operational efficiencies and explore how partners can help
- Analyse the areas of inefficiency in your financial supply chain, understand what the implications might be in terms of compliance with late payment regulation and ongoing e-invoicing efforts, and explore how cloud-based solutions can help – across both payments and the financial supply chain

VOICE OF THE CORPORATE

"SEPA implementation for AkzoNobel has led to more efficient account reconciliations for our SDD payments, lower IT costs, increased scale of automatic processing, reduced number of bank accounts and banking relations, easier centralisation of our cash management, and increased business opportunities across the SEPA region."

GERWIN BRAAM, SENIOR BANK MANAGER AT AKZONOBEL TREASURY

"We know how important small businesses are to the UK economy and how critical prompt payment is to their cash flow. Action to strengthen the Prompt Payment Code will come as welcome news to the entire UK business supply chain. Critically, the Code aims to move the UK to a 30-day payment environment. Whilst it remains voluntary, it gives businesses the opportunity to advertise concern for their suppliers' welfare and distinguish themselves from their competitors. This creates a commercial advantage for businesses that improve their payment terms, over those that are benefiting from imposing unreasonably long terms at the expense of their suppliers."

MILES GABRIEL, PROMPT PAYMENT ADVISORY BOARD

05

TAKING CONTROL: STRATEGIES TO TURN COMPLIANCE INTO COMPETITIVE ADVANTAGE

The value of cloud-based services for corporates is well-recognised: exploiting services in the cloud brings efficiency, cost and agility benefits for corporates when compared to implementing the technology solutions in-house.

The extensive compliance challenges outlined in this paper add extra weight to the argument in favour of utilising cloud providers; being able to rely on a trusted partner to provide support in the critical areas impacted by internal and external threats, regulation and industry initiatives goes a long way towards alleviating the compliance burden for corporates, while also enabling them to quickly and cost-effectively capitalise on opportunities opened up by market-driven change.

Given the rapid pace of change, it is important for corporates to select a provider with a proven commitment to staying on top of – and ahead of – market developments. Other key characteristics to look for in a trusted partner include:

- **The ability to embed internal controls and flexible entitlement management in cloud-based solutions**. This brings peace of mind, control and visibility, and ensures compliance with regulations such as Sarbanes-Oxley which enforce segregation of duties, control limits and comprehensive reporting. It enables the provision of better management and audit information, reduces reliance on staff knowledge, minimises the costs of process inefficiency and manual intervention, allows staff to be redeployed on more value-added tasks and mitigates reputational risk.

- **World-class security and resilience**. Look for a provider with a proven 'security first' approach (physical, human, digital), the ability to ensure an 'always on' infrastructure, efficient and fast connectivity and watertight data protection policies and procedures. This will help to mitigate security threats. In addition, corporates can leverage the investment of the provider in any new security measures the market requires – such as the TLS/SHA-2 requirements of Bacs.

- **Comprehensive fraud management capabilities**. The range of fraud risks impacting corporates – internal, external, cyber – is so extensive and the challenge of managing them so severe that this is a critical area in which corporates need support from trusted providers. Any partner chosen should be able to demonstrate a suite of capabilities to prevent fraudulent activity, providing protection against cyber-attacks, insider threats, web and mobile-based fraud and payment fraud to name just a few.

- **A commitment to enable connectivity to multiple banks using industry standards**. The shifting banking landscape and ongoing industry efficiency efforts mean corporates need to keep their options open when it comes to their banking relationships and how they communicate across their financial supply chains. As a consequence they need a cloud provider with solutions that enable multi-bank, multi-protocol and multi-network connectivity, and which supports all relevant and emerging electronic messaging standards, including ISO 20022.

- **A portfolio of services that is proven to evolve ahead of corporates' developing requirements**. The timely availability of cloud solutions that help corporates anticipate potential future compliance challenges – such as sanctions filtering solutions to support anti-money laundering efforts – make it straightforward for corporates to get ahead of possible future legislation and to already mitigate against the possible reputational risk of instructing payments to be made to sanctioned entities. Corporates should look for a provider with a clear commitment to anticipating their needs and being ready in advance.

- **The ability to underpin next generation payment and working capital management approaches**. With SEPA being a catalyst for the creation of payment factories and bank regulation such as Basel III potentially causing a shift in the types of services corporates can easily access from their banks, corporates have a growing need to improve the sophistication of their approaches to payments and maximise efficiency in working capital management. Trusted partners able to offer payment factory and sweeping and pooling solutions can help.

- **Leading edge AP automation capabilities**. With increasing focus on e-invoicing, corporates must move away from paper-based invoice processing and all the inefficiencies it implies. The benefits of automating the AP function are manifold – reduced processing costs, accelerated invoice approval times, improved cash management, strengthened supplier relationships and improved visibility and audit capabilities – and the easiest way for corporates to get up and running quickly and cost-effectively with automation of the invoice function is via a trusted partner with proven services in this area.

- **A full suite of AP and payments automation solutions in one place.** Leveraging the cloud for invoicing automation and payments factory functionality is especially fruitful for corporates if they can access these solutions from one provider in an integrated way – thus maximising the gains they make in efficiency, control and visibility over these vital functions, while also sharing the challenge of compliance related to these activities with their trusted partner.

In short, a cloud provider with the right credentials, solution set and strategy can take a great deal of the compliance strain for corporates, freeing them up to focus on their core business activities.

06
CONCLUSION

As this paper has described, compliance in its broadest sense is a major priority for – and drain on the resources of – corporates, in addition to BAU and their ongoing need to focus on their business development and profitability.

The intense focus in the industry as a whole on fraud, cyber-crime and financial crime is impacting corporates. They need to have a full understanding of the threats they face and to create a strong set of protections against them. Crucial to this is improving internal controls – taking full advantage of the power of the software they are using to embed rules and processes and enforce these limits and controls – and leveraging the latest technologies to ensure security.

Increasingly, in order to protect themselves from reputational risk and anticipating the extension of relevant rules to cover their activities, corporates are putting in place systems to ensure they can adhere to regulations around money laundering and to respect financial sanctions.

Corporates are also impacted by the changes in the regulatory environment in which their banks operate. Although regulations like Basel III and PSD2 primarily target financial institutions, they also have implications for corporates, in some cases creating challenges, in some cases opportunities. Corporates must both understand the changing regulatory environment for banks and formulate and execute business and technology strategies to accommodate the impact on their businesses.

Ongoing efforts to improve operational efficiency in the payments and the financial supply chain also require corporates to respond, to ensure they reap the maximum benefits from initiatives such as SEPA and e-invoicing, and comply with regulation around late payments.

In the face of this broad range of compliance challenges – and opportunities – leveraging cloud solutions is a highly viable and relevant option for corporates. Tapping into secure cloud-based solutions, which cover all aspects of payments and financial supply chain, allowing trusted providers to shoulder some of the strain of the technology change required, and mutualising the cost of adhering to regulatory, legal and security requirements, offers corporates an opportunity to minimise the cost and effort of compliance with the gamut of 'change drivers' impacting their businesses.

Corporates can gain and maintain control, focus on their business growth, minimise the challenges of compliance and maximise the benefits, enabling compliance to be converted into a competitive advantage rather than simply a burden.

07

APPENDIX A

SOME KEY REGULATIONS AFFECTING BANKS AND CORPORATES

A TIMELINE THROUGH THE YEARS

YEAR OF ENACTMENT	
2002	• Sarbanes-Oxley Act
2004	• Basel II
2005	• Market Abuse Directive (MAD)
2006	• Companies Act
2007	• Markets in Financial Instruments Directive (MiFID II)
2008	• Emergency Economic Stabilisation Act
2009	• Solvency II Directive
2010	• Dodd–Frank Wall Street Reform and Consumer Protection Act
2011	• EU Directive on Combating Late Payment in Commercial Transactions
2012	• European Market and Infrastructure Regulation (EMIR) • Financial Services Act
2013	• Financial Services Act • Basel III • Capital Requirements Directive IV • Capital Requirements Directive IV / EU's Capital Requirements Directive (CRD4) • EU Transparency Directive Review • Financial Services (Banking Reform) Act • Foreign Account Tax Compliance Act (FATCA)
2014	• EU e-Invoicing Directive • Financial Transaction Tax • Market Abuse Regulation (MAR)
2015	• New EU Data Protection Directive
2016	• Market Abuse Directive II (MADII)
2017	• Markets in Financial Investments Regulation (MiFIR)

08 ABOUT

Finextra

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology (fintech) news and information source. Finextra offers over 100,000 fintech news, features and TV content items to visitors to www.finextra.com.

Founded in 1999, Finextra Research covers all aspects of financial technology innovation and operation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide.

Finextra's unique global community consists of over 30,000 fintech professionals working inside banks and financial institutions, specialist fintech application and service providers, consulting organisations and mainstream technology providers. The Finextra community actively participate in posting their opinions and comments on the evolution of fintech. In addition, they contribute information and data to Finextra surveys and reports.

For more information:
Visit www.finextra.com, follow @finextra, contact contact@finextra.com
or call +44 (0)20 3100 3670

Bottomline Technologies

Bottomline Technologies (NASDAQ: EPAY) powers mission-critical business transactions. We help our customers optimise financially-oriented operations and build deeper customer and partner relationships by providing a trusted and easy-to-use set of cloud-based digital banking, fraud prevention, payment, financial document, insurance, and healthcare solutions. Over 10,000 corporations, financial institutions, and banks benefit from Bottomline solutions. Headquartered in the United States, Bottomline also maintains offices in Europe and Asia-Pacific. For more information, visit www.bottomline.com.

Contact for Media:
Christine Nurnberger
Bottomline Technologies
603.812.3742
cnurnberger@bottomline.com

Finextra Research Ltd
101 St Martin's Lane
London
WC2N 4AZ
United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Web
www.finextra.com