protiviti®
Face the Future with Confidence

Compliance Insights

Your monthly compliance news round up

November 2017

BCBS Issues Consultative Document on the Implications of Fintech on the Banking Industry

In August 2017, a task force of the Basel Committee on Banking Supervision (BCBS) published a consultative document assessing the impact of financial technology, or fintech, on the banking industry and the implications of fintech-driven changes on banks' business models and the agencies that regulate banks. Though the size of the fintech sector is difficult to measure, as the BCBS notes, it remains relatively small but has had an outsized impact on the financial services industry in the competition for customer relationships and customer data.

In the document, the BCBS analyzes the impact of fintech products and services on banks through five forward-looking scenarios, ranging from enhancing existing operations and legacy systems with modern customer interfaces — dubbed a "better bank" — to a fully-disintermediated bank (which refers to the full displacement of existing banks from customer financial transactions).

The common theme across these scenarios is that banks will face growing challenges in retaining and developing new customer relationships and maintaining profitability if they do not adopt and implement innovative, technological advances. The BCBS also notes that the uncertainty of technological change and customer expectations related to fintech advancements further challenge banks and bank supervisors to develop and execute effective strategies to mitigate the increased risk of safety and soundness concerns.

Following an evaluation of the implications of the opportunities created by fintech for banks and the banking system, the BCBS task force identifies 10 key observations and recommendations for consideration by banks and bank supervisors. These include the following key findings:

- The BCBS finds that the nature and scope of traditional banking risks are likely to change significantly over time as financial technologies are more widely adopted. As a result, the BCBS recommends that banks (and their regulators) consider a balanced approach to ensuring the safety and soundness of the banking system, consumer protections and compliance with anti-money laundering/counter financing of terrorism (AML/CFT) requirements while minimizing the risk of impeding valuable innovation.

- The BCBS finds that banks must contend with many risks associated with the adoption of financial technologies, including strategic, operational, cyber and compliance risks. Implementing effective governance structures and risk management processes are critical for appropriately identifying, managing and monitoring risks associated with such technologies. This includes: thoughtful strategic and financial planning, new product approval and change management processes that credibly challenge the completeness of project plans to implement financial technologies, proper evaluation of operational risks (including third-party risk management), and adaptive compliance monitoring and testing.

  In addition, the increased utilization of advanced technologies to deliver financial services comes with its own set of information technology, security and data privacy risks. Banks should ensure they have effective IT-related risk management processes to address such risks and properly support innovative products, services and technologies.

- Fintech developments present regulatory issues beyond the scope of existing supervision, including geographies and jurisdictions that challenge the current regulatory structure. Additionally, current regulatory frameworks, methods, and expertise may be outdated and not appropriately structured to effectively regulate existing and future fintech developments. The BCBS recommends that bank supervisors increase collaboration to maintain consistent and effective supervision of areas such as consumer protection, data protection, competition, and cyber-security, particularly in the supervision of global fintech firms.

  In addition, it recommends that bank supervisors continuously evaluate current regulatory frameworks against the risks associated with innovative products, consider leveraging the technology of fintech firms to improve the efficiency of supervisory activities, and review staffing and training to be informed of new technologies and business models.

The BCBS recognizes that the banking industry has undergone transformation previously as innovative financial technologies revolutionized how products and services were offered to consumers. It notes, however, that the current fintech wave is different, with lower barriers to entry and many more non-bank players. Successful financial services innovation requires the ongoing active participation of banks, fintech firms, and supervisory agencies to ensure awareness of new fintech trends and risks, and that those risks are appropriately mitigated to protect the safety and soundness of banks, fintech firms and the financial services industry.

CFPB Issues Final Rule Regarding Payday, Vehicle Title and Certain High-Cost Installment Loans

In October 2017, the Consumer Financial Protection Bureau (CFPB) issued a final rule to implement new consumer protections related to payday, vehicle title and certain high-cost installment loans. The rule highlights the CFPB's focus on so-called payday debt traps and is meant to address unfair, deceptive and abusive practices related to the origination and servicing of certain short-term loans.

The availability and affordability of short-term, small-dollar loans (often referred to as payday loans) has been the subject of much discussion in the financial services industry given the nature of the products and services offered (typically small loan amounts, offered at high rates and with a very short-term repayment period), the institutions that offer such loans (often non-bank entities, and increasingly through online means), and the consumers who use these products services (who often cannot access credit in any other form and/or may be experiencing a temporary distressing event). The final rule is intended to address CFPB concerns that lenders that offer such loans operate business and credit models that deviate from standard practices in other credit markets.

The final rule applies to the following categories of covered loans and lines of credit:

- Short-term loans, which have a term of 45 days or less, including payday loans (usually repaid in one installment and short-term vehicle title loans, as well as deposit advance products.
- Longer-term balloon payment loans, whereby the consumer repays the entire loan amount in a single payment more than 45 days after origination or is required to make at least one payment on the advance that is more than twice as large as any other payments.

- Longer-term loans, which have terms greater than 45 days that have an annual percentage rate (APR) greater than 36 percent and a leveraged payment mechanism that gives the lender a right to withdraw payments from the consumer's account. This category includes payday installment loans (repaid in multiple installments).

Certain types of loans, even if they meet the definitions above, such as home mortgages, vehicle purchase loans, student loans, and credit cards, are excluded.

The rule implements three main requirements:

- Ability to repay requirements
    - Lenders must make a reasonable determination of a consumer's ability to repay a short-term loan or longer-term balloon payment loan. The CFPB's expressed intent behind this requirement is to require lenders to ensure that borrowers can repay the loan without the need to re-borrow. The rule prescribes the specific items that must be verified by the lender.
    - Lenders are prohibited from originating short-term loans and longer-term balloon payment loans to a borrower in succession. The rule implements a 30-day cooling off period whereby lenders cannot make a new short-term loan or longer-term balloon payment loan to a customer who has taken out three such loans within 30 days of each other until 30 days after the third loan is no longer outstanding.
    - Alternatively, lenders are allowed to lend up to $500 in lower-risk situations for an initial loan; however, they cannot then structure the loan as open-end credit or take an auto title as collateral. The rule includes provisions that lenders cannot make loans to borrowers who have already had six short-term loans, or have been in debt due to short-term loans for more than 90 days in a 12-month period.
- Requirements related to payment practices
    - The rule restricts lenders' practices of obtaining payment from covered loans borrowers to prevent repeated and unsuccessful attempts to obtain payment from a consumer's checking or savings account that may result in excessive fees. Lenders are required to provide notice to consumers prior to each attempt to collect a payment.

- After two failed attempts to collect a payment, lenders are prohibited from continued collection activities, regardless of payment channel, until a specific, renewed payment authorization is obtained from the consumer.

- Consumer reporting requirements
  - To curb certain consumer reporting abuses, the CFPB requires lenders that make covered short-term or longer-term balloon loans to be prepared to furnish consumer report information to entities that are designated as a registered information system (akin to a consumer reporting agency) under the rule. Lenders are required to report loan information concerning covered loans at consummation, updates to the information over the life of the loan, and information when the loan ceases to be outstanding to a registered information system. In addition, lenders must obtain consumer reports from a registered information system before making such loans.

Compliance with the final rule is required by August 2019. Institutions that offer covered loans to consumers should begin evaluating the impact of these final rules on their existing or planned product and service offerings and related originations and servicing processes. Institutions should follow prudent regulatory change management and project planning processes to determine whether and how they must enhance their policies, programs and systems to ensure compliance with the technical and operational requirements of the new rule.

CFPB Issues Guidance for Protecting Consumer-Authorized Financial Data

In October 2017, the Consumer Financial Protection Bureau (CFPB) issued a set of consumer protection principles related to the protection of consumers when they authorize access to their financial information for third parties to provide to them consumer financial products and services. The guidance is directed at all companies that provide, use or aggregate consumer-authorized financial information. The principles are the result of a 2016 Request for Information by the CFPB to gather feedback on industry practices and risks, as well as the CFPB's evaluation of activities such as screen scraping, where consumers input their banking information into an application or tool for use of the information by third parties.

The CFPB acknowledges that there is a developing market for services based on the customer-authorized use of financial data. Many companies, including those engaged in fintech, offer consumers and financial institutions (including banks) data-based services that require customer authorization to access consumer financial information. The CFPB cites services such as fraud screening, identity and asset verification, and bill payment among the burgeoning services offered by these non-bank providers to customers and/or financial institutions that require access to consumer financial data.

The benefits of such innovative products and services are many, including consumer access to information from multiple accounts in one step to manage finances or bill payment, or obtain financial planning advice without providing paper-based records, or obtain timely approval of a loan or purchase transaction. The CFPB notes, however, that increased consumer control of consumer data and transparency must also be weighed against the importance of privacy and information security.

The principles demonstrate the CFPB's vision for a safe and workable data aggregation market that can protect consumer data while bringing value to the market and encouraging innovation. While the principles provide neither new binding obligations on market participants nor guidance on existing consumer protection laws and regulations, they do express the CFPB's viewpoint that consumer information is to be used only to the extent that is necessary for the selected services to be performed for the consumer. Key concepts addressed by these principles include:

- A consumer should be able to timely obtain information about his/her ownership of a financial product and service from his/her provider (or service provider) and should be able to authorize trusted third parties to access his/her accounts for his/her benefit. Financial product and service agreements should not restrict a consumer's ability to access or grant access to his/her account information to a third party. Access should not require the consumer to share his/her account credentials with third parties.

- Third-party access to a consumer's financial information should be limited to the data necessary to provide the products and services requested by the consumer, and retained only as long as necessary.

- Consumers should receive clear disclosures that outline 1) the scope of the financial information that they are authorizing a third party to access, 2) the terms of access, storage, usage and disposal of their information, and 3) how to revoke data sharing permissions and dispute instances of unauthorized access. Consent should be obtained

from consumers to collect and use their data, but consumers should not be required to grant access to their financial data by third-parties.

- The use of consumer data should be transparent to the consumer. Consumers should be made aware of the identity of the third parties that are authorized to access, and are accessing, their financial information, what data is being accessed, and the use and frequency of that data.
- Consumer data and access credentials should be handled securely to protect consumers from security breaches or other misuse/harm.

The CFPB's principles will seem familiar to financial institutions required to comply with the General Data Protection Regulation (GDPR). Increasingly, regulators are focused on matters related to consumer privacy and security, and the CFPB's principles are demonstrative of the global effort to provide to consumers increased control over their personal data and regulate how institutions use and protect this information.[1]

Financial institutions and non-bank providers of consumer financial products and services that provide, use or aggregate consumer-authorized financial information should evaluate the impact of these principles on their current products and services, agreements, and third-party arrangements and systems. Companies must take steps to clearly request and obtain consumer authorization and ensure that the privacy and security of consumer financial information is obtained, as well as make transparent these practices to consumers, prevent misuse, and properly dispose of information.

Finally, as partnerships with non-bank providers are expected to increase, a more discerning and nuanced approach must be taken by institutions to manage third-party risk. This will invariably be different for each institution. Protecting consumers will require an end-to-end view of the critical processes that need to be supported by both organizational design and responsibility and appropriate governance and control methodologies, as well as having enterprise visibility of all third-party relationships and risk exposure.

[1] For further information about the GDPR, please visit Protiviti's resource center on this topic.

OCC Issues Bulletin on New, Modified or Expanded Bank Products and Services

In October 2017, the OCC released revised guidance outlining its expectations for national banks to prudently manage the risks associated with new, expanded and modified products and services (referred to as "new activities"). The timing of the revised guidance is critical given recent, rapid evolution of financial products and services, delivery methods, and entrants in the market, most notably reflected in the emergence of fintech. In the bulletin, the OCC emphasizes the importance of new activities aligning with national banks' overall business plans and strategies. The OCC also underscores the importance of responsible innovation by banks in meeting the changing needs of customers.

At the time of its original guidance in 2004, there was a period of rapid change in the industry as banks introduced new, more complex products and services to customers, and to potentially riskier segments of customers. For example, traditional mortgage products were transformed to expand access to consumers with weaker credit profiles, and provided new features such as allowing a consumer to select from alternative repayment options. The OCC acknowledges that today banks are again in a period of rapid evolution driven largely by innovations in technology, and the opportunities that they create for bringing innovative products and services to customers. These opportunities come with new risks that national banks must manage not only to operate in a safe and sound manner but also to remain competitive.

The main concepts and updates addressed in the revised guidance include:

- Management is responsible for establishing a written program that outlines the standards, responsibilities, processes and internal controls for identifying, evaluating, managing and mitigating risks associated with the new activity. The program and associated responsibilities should be commensurate with the size, complexity and risk profile of the bank and be robust enough to keep pace with the complexities of any planned activities.
    - New activities should align with a national bank's strategic plan, including its established risk appetite.
    - The risk management system should clearly address four main components:
        - Adequate due diligence and approvals before introducing a new activity
        - Policies and procedures to properly identify, measure, monitor, report and control risks

        - Effective change management for new activities or affected processes and technologies
        - Ongoing performance monitoring and review systems.
    - The board should oversee management's implementation of the bank's risk management program related to new activities.

- Banks must manage the strategic, reputation, credit, operational, compliance, and liquidity risks associated with new activities. New risk types specifically addressed in the revised guidance for banks to consider include:
    - Privacy and security of customer data.
    - Oversight of third-party service providers and partners, including fintech partners, third parties that are foreign-based; those used in the solicitation, referral, underwriting, and origination on behalf of the bank, or those that are affiliated parties.
    - Inadequate consideration of the appropriateness of services for customers and of the effect on customers of these services.

- Banks must address change management processes within its risk management program, including:
    - Input from senior management, line management, and risk management, before implementation
    - Testing of systems, processes, and technology
    - Parameters and exception reporting
    - An exit strategy limiting adverse effects in the event of flawed implementation
    - Employee training on new or modified processes.

The revised guidance highlights also the growing importance of fintech companies, and the importance of understanding the technologies that these companies offer, the associated risk and controls, and the effect that the new delivery channel will have on existing operations. In the guidance, the OCC reminds national banks that fintech companies should be included in their third-party risk management processes, particularly if offering critical activities to the bank.

Board and senior management of national banks should evaluate the revised guidance and revisit their existing policies and procedures related to the risk management of new activities to ensure that they address the OCC's expectations. In doing so, they should also ensure that they are up-to-date on the technological changes that are transforming the industry so they can develop effective strategies reflective of the new environment and the risks associated with it. Given the interrelatedness, change management and third-party risk management programs should also be evaluated to address the guidance regarding new activities.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®