Bloomberg Law

Overview

Doing Business in Europe During the Pandemic– Key Legal Issues for U.S. Fintech Businesses

Gina Conheady, A&L Goodbody

Doing Business in Europe During the Pandemic– Key Legal Issues for U.S. Fintech Businesses

Contributed by Gina Conheady, A&L Goodbody

This overview highlights some of the key practical legal considerations that U.S. fintech businesses should think about as they manage the impact of the coronavirus pandemic, for their European business and operations.

Background

In the last number of years, many U.S. financial technology or fintech businesses have experienced rapid growth. With many of their technologies being borderless by nature (and plenty of investor funding available to burn), this has frequently meant expanding into new geographies beyond the U.S.

The European Union, with its market of 500 million consumers, will often be the logical first stop for a fast-growing U.S. fintech when it comes to international expansion. Newer generation disruptors like Stripe, Coinbase, and most recently Plaid, have all made significant investments in their EU operations in the last number of years, joining join fintech "incumbents" like PayPal and First Data, which have had operations in Europe from as early as 2007 and 1991 respectively.

While fintech technologies are frequently borderless by nature, the laws and regulations that apply to them are not. As the Covid-19 pandemic gathers pace across the globe, U.S. fintech businesses of all sizes and scale must consider the impact of the crisis not just for their domestic operations, but for every jurisdiction in which they do business.

Managing EU Regulatory Compliance in a Global Pandemic

Within the EU, like in the U.S., there is no specific regulatory framework that applies to fintech businesses as a class. Whether a business is regulated at either EU or member state level depends on the specific nature of the activities that are carried on by the fintech business and whether these include any regulated financial services.

The broad categories of financial services that are regulated under EU law include banking and deposit-taking, payments (including account information services, payment initiation services and e-money issuance), investment firm activities and services, fund management, insurance and pensions. While the regulatory requirements applying to these businesses vary depending on the sector and activities, most businesses falling within these categories are subject to EU regulatory rules around:

- Prudential requirements, including capital and liquidity requirements
- Governance and internal controls
- Data protection
- Conduct of business requirements
- Consumer protection
- Money laundering, terrorist financing and other financial crimes
- Business continuity
- Market integrity

For U.S. fintechs doing business in the EU, achieving regulatory compliance can be complex at the best of times, not least because the rules and applicable requirements can vary across member states. However, against the backdrop of a global health pandemic, where working from home (WFH) arrangements have become the new normal, compliance becomes all the more challenging. Along with the practical and logistical difficulties of WFH (for example, the need for "wet ink" signatures on regulatory filings, closure of registries, etc.), businesses and their customers are exposed to a heightened risk of fraud and other threats from bad actors seeking to capitalize on coronavirus-driven vulnerabilities. On top of this, cash flow issues can place constraints on meeting liquidity thresholds; and potential supply chain failures, compounded by employee absences, can threaten business continuity.

European regulators have been recognizing the heightened challenges placed on the financial services sector because of the Covid-19 pandemic. A number of regulators have indicated that they may relax certain requirements to allow financial services businesses to focus their efforts on business continuity. At the EU-level, the European Banking Authority (EBA) announced in March that it would postpone a scheduled EU-wide stress test exercise on the banks falling within its remit to 2021 to allow them "to focus on and ensure continuity of their core operations, including support for their customers." A number of other regulatory deadlines were similarly postponed later in the month.

The EBA recommended that national supervisory authorities within the EU "make full use, where appropriate, of the flexibility embedded in the regulatory framework to support the banking sector" including by planning supervisory activities (such as on-site inspections), in a "pragmatic and flexible way", and "possibly postponing those deemed non-essential." It also advised them to give banks some "leeway" in the remittance dates for some areas of supervisory reporting.

At member state level, national regulators are following the EBA's lead. For example, the U.K. Financial Conduct Authority (FCA) announced in late March 2020 that it would be delaying or postponing activity "which is not critical to protecting consumers and market integrity in the short-term" to allow regulated businesses to focus on supporting their customers. In a similar vein, on April 1, 2020, BaFin, the German financial authority, announced that it would "make full use" of the considerable flexibility in financial supervision provided for in the existing legal framework "in line with the relevant recommendations of the EU regulators and supervisors, as well as international standard-setters."

While the guidance emanating from EU regulators indicates that they may take a flexible and pragmatic approach to certain aspects of regulatory compliance during the pandemic in order to allow regulated businesses to focus on business continuity concerns, it is nevertheless clear that they still expect regulated businesses to take compliance seriously. The FCA in its statement emphasized that regulated firms must "take all reasonable steps to meet the regulatory obligations which are in place to protect their consumers and maintain market integrity" and warned that firms must have robust contingency plans in place. Similarly, the EBA has emphasized that there is "no flexibility in relation to consumer protection."

With that in mind, U.S. fintech businesses that are subject to regulation in the EU should ensure they remain vigilant in relation to EU regulatory compliance as the pandemic evolves, and existing policies and processes should be continually stress-tested in light of the changing backdrop. Businesses should also continue to monitor and follow any new guidance issued by their applicable EU and/or member state supervisory authorities.

Board Oversight of EU Operations

For the fintech sector, which was largely born in the aftermath of the 2008 financial crisis, this may be the first time that their founders and executive teams have had to face a bear market, let alone deal with a recession or manage the human impact of a health pandemic.

For many U.S. companies with international operations, founders, as well as members of the C-suite, will frequently sit on the boards of many international entities. While these executives may be deeply focused on managing the impact of Covid-19 close to home, it is important to remember that where they also sit on boards of international entities, they will also be subject to legal duties with respect to those entities. Particularly in a time of crisis, it is important to show that the board has exercised those duties and provided the requisite level of oversight with respect to the management of the crisis at local country level.

Directors' Duties and Board Meetings

Within the EU, there are certain areas of law that are heavily regulated at EU level - for example, the area of data privacy. There are other areas where EU law sets out general principles and minimum standards, but, generally speaking, leaves a large margin of discretion with the EU member states to fill in gaps. Company law falls in the latter category: EU law sets out some general requirements, in particular around transparency and disclosure, but for the most part, the regulation of companies (including rules relating to board oversight) is a matter that is left to the discretion of member states. That said, for most EU member states, board oversight is typically exercised and evidenced by holding (and documenting) regular board meetings.

While the rules relating to board meetings will vary from country to country, most European jurisdictions allow for virtual meetings and/or written board decisions. At this stage, any U.S. company with an entity or entities in Europe should be confirming the applicable board oversight requirements with local counsel. In response to the travel bans in place in most jurisdictions, they should also be working with local counsel to convene virtual board meetings and to document board decision-making, as appropriate. Regularly holding meetings (virtual or otherwise) and documenting board decision-making will be critical in demonstrating that the board exercised appropriate oversight, particularly where there may be any risk of insolvency at either group or entity level.

Tax Residency

Many U.S. companies have engaged in tax planning as part of their European expansion. With travel bans currently in place across the globe, it is important to consider the tax impact, if any, that may arise from directors not being able physically to attend international board meetings. For example, many jurisdictions operate a "central management and control" test which looks to where the strategic control of the company is exercised to determine the international subsidiary's tax residence. The location of board meetings and board of directors' decision-making is typically a key factor in determining "central management and control."

Some local tax authorities may (and have) decided to relax their policies around management and control and tax residency for the duration of the crisis. This happened in Ireland in March, for example, where the Irish Revenue Commissioners issued guidance indicating that where an individual director is unable to travel to Ireland to attend board meetings because of the Covid-19 related travel restrictions, it will not view this as impacting on the Irish tax residence status of the company. Similar statements were subsequently issued by the UK's HM Revenue & Customs (HMRC), as well as the Organisation for Economic Cooperation & Development (OECD), at the international level.

Board Oversight for Regulated Fintech Businesses

In addition, regulated fintech businesses should consider any guidance or policies issued by their respective regulator at EU or local member state level around the holding of virtual meetings and board oversight during the pandemic. They should proactively engage with regulators if any issues are anticipated.

Managing EU-Based Employees and Working from Home

At this point, most European countries are in full lock-down mode and WFH has become the new normal. This raises challenges across all business sectors, and fintech is no exception.

Essential Services Exceptions

Like the U.S., most European governments have made exceptions to their stay at home policies for businesses that provide "essential services." Generally speaking, businesses that carry out essential services may remain open and employees that provide "essential services" on behalf of employers may continue to go to work. While the rules will vary from EU member state to member state, most jurisdictions regard at least some forms of banking and financial services as essential services.

While this may not be relevant to many fintech businesses -particularly those that operate a purely online model and may be able to adapt to WFH arrangements with relative ease - some fintech businesses may need to maintain a skeleton staff onsite in order to ensure business continuity. Equally, for the small number of consumer-facing fintech businesses that incorporate bricks and mortar outlets into their business models, they may be wondering whether they can keep those outlets open to customers. To determine whether this is permissible, a country-specific analysis will be required determine the applicable rules set out in any government order issued by the particular EU member state.

If a fintech business does qualify for an exception to WFH in a particular jurisdiction and employees are required to continue to work onsite for business continuity, the business should consider and identify which employees it regards as essential to achieving this. It should also confirm whether the relevant government order imposes any specific requirements that employees must meet in order to fall within the exception (for example, in Ireland, essential employees are required to carry an employer ID or letter from their employer designating them as essential employees, together with a second form of ID).

In terms of the premises itself, it will be important to put in place adequate safeguards to reduce the risk of essential employees or customers (if applicable) contracting Covid-19. Insurance policies should also be reviewed to confirm coverage and potential exposure in the event of an infection linked to the continued operation of the business (especially where the categorization of the business as essential may have fallen in a "gray" area).

Whether or not employees will continue to go to work for the duration of a lockdown, U.S.-headquartered fintech businesses should ensure that there is a coronavirus response team in place on the ground in the local jurisdiction. This team should be responsible for monitoring local developments, including any changes to government recommendations and orders. They should be ready to respond quickly and in time zone as matters evolve, particularly if any employee at a local office appears sick or presents other risk factors.

Cybersecurity Risk

WFH arrangements mean that businesses of all sizes and scale are now vulnerable to cybersecurity threats and potential data breaches like never before. Given the nature of the activities carried on by fintech businesses, and the wide range of sensitive personal data held processed by them, businesses in this sector are likely to be especially attractive targets to malicious actors.

An example of this threat playing out occurred on March 20, 2020, when a London-based fintech company, Finastra, announced that it had been the target of a ransomware attack, forcing the company to take its IT operations offline.

Finastra is one of the biggest names in fintech, with revenues of $1.9 billion. According to their website, they provide technology and software architecture to over 9000 customers, including 90 of the top 100 banks globally. In other words, Finastra plays a critical role in the supply chain for the delivery of financial services, by providing fundamental IT infrastructure that is relied on by financial institutions across the globe in order to deliver their services to end users.

A disruption of Finastra's service is not only a crisis event for Finastra, but also for the banks, credit unions, and other financial institutions who rely on Finastra's services to provide their respective financial services to end users—ultimately the businesses who need access to liquidity and the private individuals who need access to cash to support themselves during this pandemic. So, an interruption at one level in the supply chain can have a domino effect which, against the backdrop of Covid-19 pandemic, can have potentially far-reaching effects.

Given their role in the supply chain for financial services, it is crucial for fintechs to continually review and test their IT infrastructure for vulnerabilities and educate employees on WFH-specific cybersecurity policies and measures.

On March 3, 2020, the European Central Bank issued a notice on "contingency preparedness in the context of Covid-19," or the ECB Notice, advising (among other things) that "significant institutions" should:

- Proactively assess and test the capacity of existing IT infrastructure, also in light of a potential increase of cyber-attacks and potential higher resilience on remote banking services
- Assess risks of increased cyber-security related fraud, aimed both to customers or to the institution via phishing mails etc.
- Enter into a dialogue with critical service providers to understand whether and to ascertain how services continuity would be ensured in case of a pandemic

While the ECB Notice is addressed specifically to "significant institutions" (i.e., the large EU-based banks that fall within the ECB's supervision), the approach set out in the ECB Notice is likely to be largely followed by national regulators across Europe in relation to the broader categories of financial service providers falling within their supervisory remit. That being the case, all regulated fintechs doing business in the EU (and beyond) would be well advised to take note of the recommendations.

Fintech businesses should also be mindful of the obligations imposed on them by the EU General Data Protection Regulation, as well as any related guidance issued by the European Data Protection Board and/or by national data protection agencies in the jurisdictions in which they operate. Initial guidance issued by both the EDPB and national authorities indicates that they appreciate the pressures placed on organizations by the coronavirus pandemic and suggests that they may take a pragmatic approach to GDPR compliance.

Accelerated Digital Adoption and Managing a Possible Uptick in New EU Business

The sudden move to social distancing and WFH has prompted rapid acceleration in digital adoption. While most public stocks have reeled with the impact of the crisis, businesses like Zoom and Peloton, who facilitate and enhance the virtual lifestyle that has become the new normal, have seen their stocks spike.

In the fintech sphere, the shift to virtual will put pressure on financial institutions, who continue to rely largely on bricks and mortar branches and traditional paper-based processes, to rapidly automate and digitalize legacy processes around customer onboarding, know-your-client or KYC requirements, etc. The unanticipated need to move quickly to digital could see more financial institutions turning to fintechs to leverage their existing suite of technologies and solutions.

With the uptick in digital adoption, coupled with a growing "anti-germ" economy, we are also likely to see a further movement away from cash in favor of digital and contactless payments. In Europe, for example, the EBA has issued a statement urging the European payments industry to increase contactless transaction limits to €50 to help with curbing the spread of the virus and several European countries have already taken action to increase national thresholds.

In that context, while Covid-19 will undoubtedly (and already has) taken its toll on the fintech sector, there may be new business opportunities for certain market players, and some may even see an uptick in business in the short or long term as a result of the evolving corona-conomy. Businesses falling in this category may be keen to get deals closed and new customers on-boarded as soon as possible to help with cashflow and future pipeline. While this may make sense, given the uncertain and challenging environment that lies ahead, the following are some important points to consider in connection with new EU-based business opportunities.

Critical Supplies and Force Majeure

Prior to agreeing to any new business commitments, businesses should critically assess their ability to deliver on those arrangements having regard to the constraints imposed by Covid-19. As noted in the ECB Notice, they should also begin a dialogue with any key suppliers on whom they will be relying for critical supplies in order to meet the new business commitments. They should confirm that those suppliers have measures in place to ensure uninterrupted supply and review their contractual arrangements to confirm their position in the event of supply failures.

Any new contracts should also be reviewed to ensure that they contain appropriate provisions around allocation of risk for supply chain failures, force majeure, impossibility, and change of law, etc.

E-Signing

The move to social distancing means that e-signing is becoming the norm for consumer and commercial agreements (to the extent that it was not already). Most fintechs are well accustomed to doing business electronically and e-signing is not likely to be a new challenge for them.

In the EU, Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, or the eIDAS Regulation, provides that an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form. While the eIDAS Regulation is directly applicable across the EU, Recital 49 allows member states to set requirements regarding which type of electronic signature may be required in which circumstances. Therefore, depending on the applicable law, there may be certain categories of documents where a simple e-signature will not be sufficient. An example of the type of document that may require additional execution formalities is a document that transfers an interest in real property (which could be relevant, for example, for some online marketplace lenders that facilitate secured loans or mortgages).

Accordingly, while electronic signatures should, in principle, be acceptable in most circumstances, given the nuances that can apply to e-execution across EU member states, it would be prudent for U.S. fintech businesses to reach out to local counsel in any key markets to determine any restrictions on e-signing that may cause delays in closing new business deals, and confirm available work-arounds, if appropriate.

Anti-Competitive Conduct

The economic and social uncertainty caused by Covid-19 may increase the temptation for businesses and their employees to find ways to cooperate with their competitors or third parties to restrict competition (e.g., by agreeing prices with others in the industry). There may also be opportunities for businesses and their employees to coordinate their behavior through

trade associations. Equally, for businesses that find themselves on the upside of the corona-conomy, there may be some temptation to engage in price-gouging (similar to what we have seen in relation to hand sanitizers in the in the health and sanitation sector) or other unfair practices.

Under EU antitrust laws, it is an offense to enter into an anti-competitive agreement or to abuse a dominant position. A breach of these two key principles can lead to fines (up to the greater of €5 million or 10% of worldwide turnover) and imprisonment (up to 10 years where the offence is a cartel) and other consequences such as the invalidity of agreements and damages for harm caused by such infringements. In addition, consumer protection law prohibits conduct such as misleading advertising and unfair contracts – a breach of these requirements is also an offence with significant sanctions.

The European Competition Network has issued some helpful guidance on the interplay between the Covid-19 crisis and EU competition law rules. The ECN has indicated that while it will not actively intervene in the case of necessary and temporary measures (e.g., cooperation initiatives) which are put in place in order to avoid a shortage of supply, it equally will "not hesitate to take action against companies taking advantage of the current situation by cartelising or abusing their dominant position."

Therefore, vigilance by businesses and employees should continue to be exercised in relation to EU anti-trust rules. In particular, businesses should not enter into any agreement with competitors involving the fixing of prices, the limitation of sales/output, the sharing of markets/sources of supply or other actions which have as their object or effect the restriction of competition. They should avoid sharing competitively sensitive information (e.g. around pricing and marketing plans) with competitors and, importantly, refrain from any form of price-gouging or similar practices that take advantage of a dominant position.

Anti-Money Laundering/KYC

Lastly, regulated fintech businesses that are subject to anti-money laundering and KYC requirements should ensure that they have appropriate digital processes in place to allow them to carry out new customer identity checks securely and efficiently.

The global AML standard-setting body, FATF (the Financial Action Task Force), recently issued Guidance on Digital Identity, and a related statement in which it encouraged "the fullest use of *responsible* digital customer onboarding and delivery of digital financial services in light of social distancing measures".

Several European regulators have indicated that regulated businesses can take a flexible approach in this regard, with the FCA even suggesting that the use of "'selfies" or videos" to check the identity of clients may be acceptable.

Businesses should ensure that whatever method they use, their processes are secure and compliant with the FATF Guidance, as well as other guidelines or standards set by their applicable EU or local-level regulators. They should also ensure that any personal data that they obtain through their KYC processes is held and processed in compliance with the General Data Protection Regulation (GDPR).

Staying Afloat: Capital and Liquidity Management

At this point, businesses should have already carried out a detailed assessment of their current and projected financial position in light of the coronavirus, and cash conservation and maximization strategies should be well underway. For U.S. businesses with international operations, any such strategies should be considered at entity as well as group level in the context of the board oversight process mentioned previously. Any measures being taken should be carefully considered and documented.

Regulated Businesses

In addition to general cash and liquidity needs, regulated businesses must also bear in mind the capital and liquidity requirements that apply to them under their respective regulatory regimes. A number of regulators across Europe have indicated a willingness to relax liquidity requirements in the context of the coronavirus crisis and the ECB has advised that banks falling with its supervisory authority can fully use their capital and liquidity buffers. However, as a practical matter, if a regulated fintech business believes its liquidity is likely to fall below applicable regulatory thresholds, it should proactively engage with its respective regulator as early as possible.

From a capital conservation perspective, the ECB has recommended that, until Oct. 1, 2020, banks within its supervisory authority should refrain from paying dividends or implementing share-buy backs, with a view to conserving capital and ensuring it is available to "support the real economy and absorb losses." This recommendation was issued to national supervisory authorities and is expected to be rolled out by regulators at national level in relation to other regulated businesses falling with their remit. In that context, any liquidity strategies being considered at the U.S.-level that will involve repatriating cash from EU subsidiaries (through dividends, share buy-backs or other cash extraction mechanisms) should be carefully considered. Any such strategies should be implemented with the utmost caution, and only following consultation with local and U.S. legal counsel, particularly if there are also liquidity concerns at the EU-entity level. The latter applies to both regulated and unregulated fintech businesses alike.

Government Supports To help bolster their liquidity within the EU, U.S. fintech businesses should bear in mind that there may be financial supports available to them at both the EU and member state level. At EU-level, the European Commission has announced the Corona Response Investment Initiative, under which it will make €37 billion available for crisis response to help with supporting particularly vulnerable sectors, such as small-to-medium-sized enterprises.

Financial support packages frameworks are also being rolled out at national level across EU member states. In the U.K., the government has announced a £330 billion package of bailout loans, alongside wage subsidies which can be availed of by businesses. A new lending scheme from the Bank of England has also been introduced, which will provide funding to business by purchasing commercial paper of up to one-year maturity, issued by firms making a "material contribution" to the U.K. economy.

France is rolling out three financial aid schemes, two of which will enable Bpifrance to provide state guarantees on commercial loans and credit lines for enterprises with up to 5,000 employees. The third is a scheme to provide state guarantees to banks on new loan portfolios for all types of companies. Combined, all three schemes are expected to provide more than €300 billion of liquidity support for companies affected by Covid-19.

Similarly, Ireland has introduced a €200 million working capital scheme for eligible businesses, including loans of up to €1.5 million at reduced rates. A further €200 million package for enterprise supports including a rescue and restructuring scheme for vulnerable but viable companies has also been introduced.

Other EU countries have rolled out similar initiatives, some of which may be available to U.S. fintech businesses with respect to their European operations, depending on the facts and circumstances.

Exiting the EU

As the impact of lockdowns, decreased consumer spending and loan defaults continue to take their toll on the financial services and fintech sectors alike, certain U.S. fintechs may reach the decision that it is no longer feasible for them to continue to do business in the EU.

In the event a U.S. fintech business decides to exit the EU, there are several factors to bear in mind. First, unlike in the U.S., EU member states do not recognize the concept of employment at will. To the extent a fintech business has employees in the EU, there will be employee consultation and notification processes that must be observed in order to lawfully implement redundancies. Where terminations are envisaged, local counsel in each EU jurisdiction in which the employees are located should be consulted as early as possible to confirm what local processes must be complied with.

To the extent that a U.S. fintech has incorporated a subsidiary or branches in the EU, these will need to be wound down. Again, the process to unwind these will vary from member state to member state and advice should be sought from local counsel in the relevant EU jurisdiction. If the wind-down happens in insolvent circumstances and the local entity is unable to pay its debts as they fall due, it will be subject to the insolvency laws that apply in the relevant EU jurisdiction. Most jurisdictions impose some form of personal liability for directors of insolvent companies who are found to have knowingly carried on the business of the company in a reckless or fraudulent manner (although the U.K., for example, has indicated that the applicable rules will be relaxed during the pandemic, and other member states may adopt a similar approach). Nevertheless, this again underlines the importance of holding and documenting regular board meetings and ensuring the board maintains an oversight role with respect to international as well as domestic matters, particularly as cash flow issues begin to escalate.

For regulated businesses, the closure of EU operations will involve an additional lawyer of complexity as advance engagement with the local regulator will be required before it will be possible to formally cease business. Regulators will seek to ensure that customers are not adversely impacted or disadvantaged by the closure, particularly where customer assets such as deposits, other funds, or financial instruments, are held and need to be returned.

Conclusion

The deep and sudden economic shock of the Covid-19 pandemic has left businesses reeling. While the full impact of the pandemic on the global fintech sector is uncertain at this point (and may be uncertain for several years), it is clear that there are tough times ahead, both domestically and internationally. Implementing appropriate legal and regulatory compliance strategies (including robust business continuity planning and risk mitigation processes) at both the domestic and international level will be a critical factor in ensuring that a fintech business is well positioned to successfully navigate the challenges that lie ahead.