Lessons From Europe

What Money Transmitters and Regulators Can Learn from Europe’s Successes and Mistakes

Erin Fonte
Dykema

Brenna McGee
Dykema

Ben Steyn
TransferWise
Disclaimer

• The opinions expressed in this presentation are solely those of the presenter and do not necessarily reflect the opinions of Dykema or TransferWise.

• This presentation is an educational tool that is general in nature and for purposes of illustration only. The materials in this presentation are not exhaustive, do not constitute legal advice and should not be considered a substitute for consulting with legal counsel. Neither Dykema nor TransferWise has obligation to update the information contained in this presentation.
Erin Fonte

- Member and FinTech/payments lawyer with Dykema Gossett, PLLC
- Head of the Financial Services Regulatory and Compliance group and the FinTech, Payments and Digital Commerce group, and Co-Head of the firm’s Privacy and Data Security group
- Advises financial institutions and FinTech companies regarding mobile banking, mobile payments and mobile/online lending products and services, including regulatory and licensing issues
- Extensive experience in representing her client base with regard to software as a service and cloud computing agreements for third party vendors, including core banking service providers and other financial services technology vendors, and has advised institutions regarding FinTech companies as partners and as banking clients
- Member of the Federal Reserve Board’s Faster Payments Task Force.
- Frequently writes and speaks on FinTech, payments, and privacy/data security issues. Twitter: @PaymentsLawyer
Brenna McGee

- Attorney in the Austin office of Dykema Gossett, PLLC
- Brenna advises fintech companies, money transmitters and alternative payment providers on the permissibility and structure of new activities, including conducting due diligence reviews; analysis of federal money services business registration and state money transmission licensing requirements; and preparing customer-facing documentation and disclosures
- Brenna also assists banks and other financial institution clients with a variety of regulatory and corporate matters, including the preparation of regulatory applications and notices; digital, mobile banking and deposit products; mergers and acquisitions; treasury management and payment processing arrangements; and technology, outsourcing and vendor contracts
- In addition, Brenna represents banks and fintech companies in government investigations and enforcement actions
- Prior to joining Dykema, Brenna was an Assistant General Counsel at the Texas Department of Banking. Brenna is a member of the Texas Bankers Association’s inaugural “Future of Banking” Task Force. She previously served as the Chair of the Financial Institutions Section of the Austin Bar Association
Ben Steyn

- Ben is the Head of Compliance and the Money Laundering Reporting Officer at TransferWise Limited, an international money transfer platform, where he is responsible for the organization’s global compliance program.
- Ben joined TransferWise in 2014, and built up a compliance framework to support its rapid international expansion into the US and Canada, Latin America and APAC region.
- Ben currently leads a team of global Compliance Officers, who work with regulators and law makers in their respective jurisdictions to further the TransferWise mission of providing customers with transparent, convenient and eventually free money transfer and payments services.
- Before joining TransferWise, Ben was Head of Compliance at international payments organization, Skrill.
The EU Passporting System

- The EU passporting system for banks and financial services companies – including payments companies and money transmitters – enables firms that are authorized in any European Union (EU) or European Economic Area (EEA) country to trade freely in any other with minimal additional authorization.
- These passports are the foundation of the EU single market for financial services.
The EU Passporting System

How does passporting work?

A ‘passported’ UK based bank has broad and well understood rights. It can:

- Provide its customers with the widest range of banking services across the UK and all 27 EU countries.
- Establish a branch in any other EU country from which it can offer cross-border banking services across all other EU countries.
- Do so efficiently, without duplication and at low cost.
The EU Passporting System – Background

- All member states of the European Union are part of the EU single market; the single economic area created by the integration of the markets of the EU states. Goods circulate freely in this market, and businesses established inside it have wide-ranging rights to sell products and services in any part of it. Over time, the EU states have harmonized their rules for many products and services in order to facilitate this trade and to guarantee common standards across the EU.

- For over twenty years the scope of the EU single market has increasingly extended into trade in financial services. The foundation of this has been the development of a single EU rulebook for financial services and the increasing harmonization of standards of financial regulation and supervision across the EU.
The EU Passporting System – Background

• Confident in this shared standard, EU states have opened their national markets to the provision of financial services directly from other EU states, or by making it easier to establish branches (instead of more complex and costly legally separate subsidiaries) of banks and financial services firms from other EU states.

• Once a bank or financial services firm is established and authorized in one EU country, it can apply for the right to provide certain defined services throughout the EU, or to open branches in other countries across the EU, with relatively few additional authorization requirements. This pan-EU authorization is its financial services “passport.”
The EU Passporting System – Why?

• The EU passporting system is built on the assumption that banks and financial services firms authorized anywhere in the EU will have met the same standards, and thus should in effect be treated as if they were locally authorized.

• This is reinforced by a very high level of regulatory cooperation between national supervisory authorities in the EU, including the merging of some supervisory functions for EU states participating in the banking union.
The EU Passporting System – Regulation

• Once its passport is obtained, a payments company continues to be regulated and supervised by its home state regulator.

• Host state regulators can regulate the conduct of business of passported branches. However, their powers to regulate the conduct of business of passported services offered on a cross-border basis are narrower.
The U.S. Licensing Regime

• In the U.S., the states – rather than the federal government – are the primary regulators of money transmitters.

• With the exception of Montana, every state now requires businesses performing money transmission as a service for customers in their state to be licensed.

• U.S. money transmission regulations are not uniform. Each state has independently passed a statute that generates its regulatory regime. Only 12 states and territories have adopted the uniform model law. In every other state, key aspects of the law differ, such that the non-uniformity extends to fundamental features, including to the definition of money transmission itself.
The U.S. Licensing Regime – Problems

• The U.S. licensing regime makes operating an internet-based money transmission business particularly difficult. These companies do not operate on a state-by-state basis; they are available nationally as soon as their website goes live. But because licensing is state-by-state, an internet MT business cannot offer services to the general public until it firsts obtain licenses in every jurisdiction.

• That may not be such a problem if getting MT licenses was easy. But obtaining all 53 state licenses is onerous. It takes significant time and money.

• The current regulatory framework may hinder the development of innovative financial products that promise substantial consumer benefit because the barriers to entry are too high.
MT Licensing for Cryptocurrency Businesses

Consensus

State MTL Laws
- NO (13)
- YES (9)
- UNCLEAR (3)
- LEGISLATION (5)
- NO RULING (20)
- MTL COMPACT (7)
Lessons from Europe for Passporting

- U.S. regulators recognize the current system isn’t perfect
- State regulators are taking steps towards license reciprocity through CSBS’s Vision 2020 initiative:
  - In February, seven U.S. states agreed to a multi-state compact that standardizes key elements of the licensing process. If one state reviews key elements of a license application, then other states agree to accept those findings.
  - This multi-state compact is just the first step for state regulators in moving towards an integrated, 50-state system of licensing and supervision for MSBs by 2020.
Lessons from Europe for Passporting

- U.S. federal regulators are approaching the multi-state licensing issue in a different way
- In July 2018, the OCC announced it will begin accepting applications for national bank charters from non-depository fintech companies, including money transmitters. This would preempt state licensing laws and allow immediate access on a national basis
- This approach is supported by Treasury, which said in its recent Fintech Report, “Treasury encourages the Office of the Comptroller of the Currency to further develop its special purpose national bank charter, previously announced in December 2016. A forward-looking approach to federal charters could be effective in reducing regulatory fragmentation and growing markets by supporting beneficial business models.”
Lessons from Europe for Passporting

- Treasury is not opposed to state-based licensing. The same Fintech Report says, “State regulators play an important and valuable role in the oversight of nonbank financial services firms. Treasury supports state regulators’ efforts to build a more unified licensing regime and supervisory process across the states.” The Report supports state harmonization of MT laws, including through the adoption of a model law, improvements to NMLS, wider use of multi-state exams, and the Vision 2020 initiative.

- However, Treasury wants to see quick action from state regulators. The Report says, “Treasury recommends that if states are unable to achieve meaningful harmonization across their licensing and supervisory regimes within three years, Congress should act to encourage greater uniformity in rules governing lending and money transmission to be adopted, supervised, and enforced by state regulators.”
The UK Fintech Regulatory Sandbox

- A regulatory sandbox is a structure set up by a financial regulator to allow companies to conduct small scale, live testing of products and services in a controlled environment prior to full-scale public release.
- Sandboxes are designed to create a safe space in which firms can enter the financial services market and experiment with new ideas with regulatory support and oversight. This gives the companies the ability to amend and improve their products and services based on feedback before path dependency sets in, and before they have invested significant funds.
The UK Fintech Regulatory Sandbox

- In 2015, the United Kingdom’s Financial Conduct Authority (FCA) announced the world’s first fintech “regulatory sandbox,” which officially launched in May 2016.
- The FCA’s sandbox seeks to provide fintech entities, including those in the payments and money transmission space, with:
  - the ability to test products and services in a controlled environment
  - reduced time-to-market at potentially lower cost
  - support in identifying appropriate consumer protection safeguards to build into new products and services, and
  - better access to finance
The UK Fintech Regulatory Sandbox

• Both startups and incumbents are eligible for the FCA’s sandbox, and applicants must demonstrate that they are:
  – (i) carrying out or supporting financial services business in the UK,
  – (ii) genuinely innovative,
  – (iii) have an identifiable consumer benefit,
  – (iv) have a need for sandbox testing, and
  – (v) are ready to test.

• The FCA operates its sandbox on a cohort basis with two six-month test periods per year.
The UK Fintech Regulatory Sandbox

- Over its first two cohorts, the FCA received applications from 146 firms and accepted 50 of those into the sandbox. The sandbox participants are mainly in the retail banking space, but others sought to test products and services related to insurance, pensions and retirement income, retail investing, and retail lending.

- As to innovative technology, 17 fintech firms utilized distributed ledger technology in some way. Several others tested online platforms, application programming interfaces (APIs), robo-advising, and biometrics.
The UK Fintech Regulatory Sandbox

- In October 2017, the FCA published a Regulatory Sandbox Lessons Learned Report. The report reflected on how the sandbox met its objectives over the first year of operation. The FCA concluded that the first year of operation provided an early indication that the sandbox has been successful in meeting its overall objective.
- Some notable statistics from the report are that around 90% of the FinTech firms that completed testing in the FCA’s first cohort continued toward a wider market launch following their test and that at least 40% of firms that completed testing in the first cohort received investment during or following their sandbox tests.
# FINTECH REGULATORY SANDBOXES
## AS AT APRIL 2017

A **fintech regulatory sandbox** is a regulator-driven initiative that allows businesses to test innovative products, services, business models and delivery mechanisms in a live environment. Typically, some regulatory requirements are amended to create a bespoke framework for the duration of an on-market trial.

<table>
<thead>
<tr>
<th>LIVE (in alphabetical order)</th>
<th>PROPOSED (in alphabetical order)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ABU DHABI</strong></td>
<td><strong>AUSTRALIA</strong></td>
</tr>
<tr>
<td>Abu Dhabi Global Market</td>
<td>Australian Securities &amp; Investments Commission</td>
</tr>
<tr>
<td><strong>CANADA</strong></td>
<td><strong>DUBAI</strong></td>
</tr>
<tr>
<td></td>
<td>Dubai Financial Services Authority, Dubai International Financial Centre</td>
</tr>
<tr>
<td><strong>HONG KONG</strong></td>
<td><strong>MALAYSIA</strong></td>
</tr>
<tr>
<td>Hong Kong Monetary Authority / Applied, Science and Technology Research Institute</td>
<td>Bank Negara Malaysia</td>
</tr>
<tr>
<td><strong>NETHERLANDS</strong></td>
<td><strong>RUSSIA</strong></td>
</tr>
<tr>
<td></td>
<td>Authority for the Financial Market and De Nederlandsche Bank</td>
</tr>
<tr>
<td><strong>SINGAPORE</strong></td>
<td><strong>UK</strong></td>
</tr>
<tr>
<td>Monetary Authority of Singapore</td>
<td>Financial Conduct Authority</td>
</tr>
<tr>
<td><strong>THAILAND</strong></td>
<td><strong>USA</strong></td>
</tr>
<tr>
<td></td>
<td>Bank of Thailand</td>
</tr>
<tr>
<td></td>
<td>Federal Reserve Board / Treasury Department / Securities and Exchange Commission</td>
</tr>
<tr>
<td><strong>INDONESIA</strong></td>
<td><strong>SWITZERLAND</strong></td>
</tr>
<tr>
<td>Bank Indonesia</td>
<td>Financial Market Supervisory Authority of Norway, ICT Norway</td>
</tr>
<tr>
<td><strong>NORWAY</strong></td>
<td><strong>TAIWAN</strong></td>
</tr>
<tr>
<td>Financial Supervisory Authority of Norway, ICT Norway</td>
<td>Financial Supervisory Commission</td>
</tr>
</tbody>
</table>

---

Exceptional service. Dykema delivers.
Lessons from the UK Fintech Regulatory Sandbox

• Financial regulators have recognized that compliance with strict financial regulations is often incompatible with the growth and pace of the most innovative companies. The concept of a regulatory sandbox is an attempt to address this friction and give fintech firms room to grow innovative products and services in a way that doesn’t diminish consumer protection.

• As it stands, due to the high barriers to entry, FinTech firms often begin operations without first obtaining all the required licenses or complying with all the requisite laws, which leaves consumers exposed and unprotected should such a company fail. By allowing firms to experiment with real customers in a regulatory sandbox, regulators hope to remove some of the temptation for firms to operate illegally, rely on loopholes, or take an aggressive reading of laws and rules, in order to try to fall outside the scope of regulation in their testing phase.
Lessons from the UK Fintech Regulatory Sandbox

- In March, Arizona Governor Doug Ducey signed House Bill 2434 into law, making Arizona the first state in the U.S. to enact a fintech sandbox.
- On August 3, 2018, the Arizona sandbox went live and began accepting applications.
- The Arizona Attorney General oversees the sandbox and will allow approved fintech companies to engage in the testing of products and services on up to 10,000 state residents (and as many as 17,500 residents in some instances) and for up to two years (with the possibility of an additional one-year extension) without additional licensing.
Lessons from the UK Fintech Regulatory Sandbox

• The Arizona sandbox is open to any person, therefore startups and mature firms will both be able to apply
• Notably, the Arizona Attorney General will have to consult with the applicable regulatory agency before approving an applicant, but the Attorney General retains sole authority to make the final decision on whether to admit an applicant
• Although the Arizona sandbox is a first among U.S. states, the Arizona statute notably includes a reciprocity feature that would allow sandbox participants to participate simultaneously in similar programs in other jurisdictions, with the Arizona Attorney General’s permission
• Illinois and Texas are also considering their own sandboxes
Lessons from the UK Fintech Regulatory Sandbox

- The Treasury Fintech Report also supports the creation of a national regulatory sandbox
- Treasury recommends that federal and state financial regulators establish a unified regulatory sandbox that coordinates and expedites regulatory relief to permit meaningful experimentation for innovative products, services, and processes
- Treasury says that it will work with federal and state financial regulators to design a sandbox in a timely manner
- However, if financial regulators are unable to address to cooperate, then Treasury recommends that Congress consider legislation to provide for a single process, including preemption of state laws if necessary
PSD2 and Open Banking

• In January, the Revised Payment Services Directive (PSD2) went into effect in the EU
• PSD2 is a continuation of the original Payment Services Directive, which established an EU-wide legal framework for payment services, including the information requirements, and the respective rights and obligations, of payment service users and non-bank providers. It also has increased competition and choice by facilitating market entrance for non-bank players, like money transmitters and other fintech firms
• The objective of PSD2 is to increase competition, by ending the monopoly that banks have on their customer account information and payment services
PSD2 and Open Banking

- The most notable—and controversial—aspect of PSD2 is the requirement that banks openly share their customer data with non-bank payment service providers, including fintechs.
- Until now, most banks have not allowed third party providers to access customer data directly; instead, most non-bank providers have been accessing consumer data using the consumers’ account credentials.
- This technique, known as “screen scraping,” allows the third parties to stand in the shoes of consumers and access all of the consumers’ account information.
- PSD2 forces banks to release their data in a secure, standardized form so that it can be shared more easily between authorized organizations online.
PSD2 and Open Banking

- PSD2’s implementing regulations ban standard screen scraping and require banks to create or open their APIs
- PSD2 makes it possible to pass rich customer data to third parties, who can use it to create new products. PSD2 is not an app or a service in its own right; it’s a way of facilitating data sharing
- Although banks are understandably reluctant to share valuable customer data with their competition, there is a consensus that open APIs are preferable to screen scraping as APIs offer a more secure way for banks and fintechs to share account data
PSD2 and Open Banking
Lessons from PSD2 and Open Banking

- While Europe moves forward with laws and regulations on data sharing between banks and fintech companies, data sharing in the U.S. remains informal.
- Screen scraping remains the norm and banks allow it due to market pressures and consumer demand.
- While the CFPB has the authority to pass regulations on data sharing under Dodd-Frank, it has opted not to do so thus far. In October 2017, the CFPB published a set of nine non-binding Consumer Protection Principles which affirmed consumers’ ownership rights over their financial data. But the Principles do not mandate how banks must share that data with consumers and third parties in the U.S.
Lessons from PSD2 and Open Banking

• The Treasury Fintech Report discusses secure data sharing but also does not recommend legislation.

• Treasury says that it “sees a need to remove legal and regulatory uncertainties currently holding back financial services companies and data aggregators from establishing data sharing agreements that effectively move firms away from screen-scraping to more secure and efficient methods of data access.”

• But it also goes on to say that “Treasury believes that the U.S. market would be best served by a solution developed by the private sector, with appropriate involvement of federal and state financial regulators.”
Lessons from PSD2 and Open Banking

• The current data sharing landscape in the U.S. is unsustainable. Although it may be best to have a regulator like the CFPB craft a solution, direction from Washington likely will not occur anytime soon. Yet U.S. banks and fintechs would be wise not to wait on formal data sharing requirements, given the clear trend towards open data sharing via APIs. Banks should start developing APIs now, and fintechs should be prepared to lose the ability to screen scrape, rather than wait for a PSD2-esque law to mandate it.

• For regulators, one of the key issues around data sharing remains who is liable for failing to keep customer data secure? Banks have expressed concerns that they may bear the burden of any losses arising from a breach or compromise of consumer information at a fintech. Before banks will share data via open APIs, there will likely need to be a law or other specific regulatory requirement that sets who is responsible for the security obligations and liability of shared data.
GDPR in the EU (and beyond)

- In May, the EU’s General Data Protection Regulation (GDPR) became enforceable. GDPR is a wide-ranging set of requirements regarding the treatment of personal data of individuals in the EU.
- GDPR affects all companies, individuals, corporations, public authorities or other entities that offer goods or services to individuals in the EU. For example, GDPR applies to an American company whose website is made available to people in the EU, or a US-based HR manager in an international organization that collects data centrally from EU-based applicants and employees. GDPR even applies to charities and nonprofit organizations that collect information from individuals in the EU.
GDPR in the EU – Key Items

• **Consent**: Businesses can no longer gain consent from long illegible terms and conditions, implied consent, or acquiring data for one purpose (say a newsletter) and then using it for another (say marketing). Businesses will also have to make it just as easy to opt out as it is to opt in and in the same format.

• **Right to be Forgotten**: Individuals will have the right to request that a company tells them what data they have about them, how it’s being used and ultimately, request they delete it.

• **Portability**: Companies must store data in a ‘common use and machine readable format’ because individuals have the right to withdraw their data from one processor and move it to another if they choose.
GDPR in the EU – Key Items

- **Data Breaches**: In the case of a breach, the processor must make a formal notification within 72 hours, as well as notify customers “without undue delay”
- **Privacy by Design**: Systems must be designed with privacy in mind from the outset, not as an aside or an addition
- **Data Protection Officers**: Businesses that handle large amounts of data will have to appoint (or outsource) a Data Protection Officer
- **Penalty**: 20 million Euros or 4% of a business’s annual global turnover (whichever is bigger). And consumers will also be able to claim compensation from any damages from infringements of these policies
GDPR in the EU
Lessons from GDPR

• Most importantly, if you are a money transmitter that offers services to individuals in the EU, then GDPR applies to you! Get compliant ASAP! Remember the penalty for non-compliance can be as much as 20 million euros (around $24 million), or 4 percent of your annual global turnover — whichever is a *higher* amount of money
Lessons from GDPR

• The California Consumer Privacy Act of 2018
  – Signed into law in June; effective January 1, 2020
  – Sets a new tone for data protection in the United States
  – Many similar provisions to GDPR, including the right to be forgotten and a requirement for data portability
  – Allows consumers to submit up to 2 verifiable consumer requests a year, free of charge, which may request access: to their personal information held by the business, to have their information provided to them in a portable format, and to have their information deleted
  – Requires disclosure of how data will be used, but not affirmative consent as with GDPR
Lessons from GDPR

- The California Consumer Privacy Act of 2018
  - Applies to California Residents and Only Certain Businesses: the Act only applies with respect to California residents and only applies to businesses that “do business in the State of California” and need meet only one of three criteria: (1) derives 50% or more of its annual revenue from selling personal information; (2) has annual gross revenue in excess of $25,000,000; and (3) buys, receives, sells, or shares the personal information of more 50,000 or more consumers, households or devices on an annual basis
Lessons from GDPR

• The California Consumer Privacy Act of 2018
  – Expands the definition of personal information under California law from certain categories of information to “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”
  – Consumers must be given the opportunity to opt-out from their personal information being sold or shared with third-parties and may not be discriminated against through a change in the quality or pricing of services unless the difference is reasonably related to the value provided by the sharing of the consumer’s data.
  – Third-parties who receive or buy personal information must provide consumers the same opportunity to opt-out of the further selling or sharing to further parties.
# Questions?

<table>
<thead>
<tr>
<th>Erin F. Fonte</th>
<th>Brenna McGee</th>
<th>Ben Steyn</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Member</strong></td>
<td><strong>Attorney</strong></td>
<td><strong>Head of Compliance</strong></td>
</tr>
<tr>
<td>Fintech, Payments and Digital Commerce</td>
<td>Fintech, Payments and Digital Commerce</td>
<td>and Money Laundering Reporting Officer</td>
</tr>
<tr>
<td>Financial Institutions</td>
<td>Financial Services</td>
<td>TransferWise Limited</td>
</tr>
<tr>
<td>Regulatory &amp; Compliance</td>
<td>Regulatory &amp; Compliance</td>
<td>2nd Floor</td>
</tr>
<tr>
<td>Dykema Gossett PLLC</td>
<td>Dykema Gossett PLLC</td>
<td>186-188 City Road</td>
</tr>
<tr>
<td>111 Congress Ave., Ste 1800</td>
<td>111 Congress Ave., Ste 1800</td>
<td>London, EC1V 2NT</td>
</tr>
<tr>
<td>Austin, Texas 78701</td>
<td>Austin, Texas 78701</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>Direct: 512-703-6318</td>
<td>Direct: 512-703-6319</td>
<td>Direct: +44 78450 24018</td>
</tr>
<tr>
<td><a href="mailto:efonte@dykema.com">efonte@dykema.com</a></td>
<td><a href="mailto:bmcgee@dykema.com">bmcgee@dykema.com</a></td>
<td><a href="mailto:ben@transferwise.com">ben@transferwise.com</a></td>
</tr>
<tr>
<td><a href="https://twitter.com/PaymentsLawyer">@PaymentsLawyer</a></td>
<td></td>
<td>Skype ID: bensteyn9</td>
</tr>
<tr>
<td>Erin Fonte</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Exceptional service. Dykema delivers.