Mobile payments start-ups: the need to know legal landscape

New payments companies need to be aware of the legal and compliance issues that are part of operating in two of the most heavily regulated US industries: financial services and telecommunications. Getting the legal and regulatory issues wrong can be fatal to a start-up's business model and product offering. Erin Fonté, a Shareholder and Payments Lawyer at Cox Smith Matthews, discusses the fragmented US regulatory landscape surrounding m-payments and the need to bake in compliance from the start.

New offerings for mobile AS point-of-sale (e.g. Square, GoPay by Intuit) and mobile AT point-of-sale (e.g. Google Wallet, PayPal, Isis), for example, seem to spring up daily. There are at least 40 and as many as 120 different mobile wallets currently in the US alone[1]. Mobile payments is a hot area for technology start-ups, and venture capital funds have flowed freely to start-ups touting the 'magic bullet' for disrupting the traditional payments networks and potentially making big dollars in the process. The global value of mobile payment transactions is predicted to reach $1 trillion by 2017[2], and lots of time, energy and money is being spent chasing a piece of the mobile payments pie.

Failure to comply with the laws can result in regulatory orders and enforcement actions, lawsuits, and civil and even criminal fines at both the federal and state level. Companies in this space would be wise to pay attention to these issues. There can be a lack of awareness of technology professionals regarding all of the potential laws applicable to mobile payments, and many start-ups find a company doing something similar, and decide they can do it as well - in effect modeling on other companies without knowing that their role models are also not in compliance with applicable law. Ignorance of the law is no excuse, and doubly so when you are responsible for moving people's money.

What activities will your company engage in?

This is the first fundamental question to answer in order to understand what laws, rules and regulations your mobile payments product will trigger. Laws, rules and regulations have been revised over the past few years to expand definitions to include almost any type of payments- related technology that exists now or will exist in the future. For example, the definition of 'access device' under the Federal Reserve Board's Regulation E (the rule implementing the federal Electronic Funds Transfer Act) is 'a card, code or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers.'

Federal US banking regulators (including the Federal Reserve Board and the US Department of Treasury's Financial Crimes Enforcement Network (FinCEN)), and consumer protection regulators (including the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC)) have made it very clear that regulations do not apply simply by virtue of who you are (such as whether you are a bank or non-bank), but rather apply to what you do.

Are you launching a service to help African expatriates send money home from abroad? Then you are potentially engaging in money transmission and foreign remittance, and will have to be registered with FinCEN as a 'money service business,' as well as comply with the forthcoming foreign remittance rule soon to be finalised by the CFPB.

Are you launching a service that will allow consumers to buy products now and defer paying for them for a certain period of time? If so, then you may be engaging in an 'extension of credit' and are subject to the federal Truth-In-Lending Act (TILA) and corresponding Federal Reserve Regulation Z. Are you creating a 'big data' type of service that will track, analyse and crunch information on the buying habits of your mobile payments users, including where they go and what they buy? Then you will definitely trigger federal and state privacy and consumer protection laws regarding geo-location tracking and use of personal information (including opt-in requirements).

And those are just governmental laws, rules and regulations. If any of the payment activities you will be engaged in include transmitting and settling transactions over the credit or debit card networks, ATM networks or the automated clearinghouse system, those activities will trigger compliance with the private network rules of credit card associations (e.g. American Express, Discover, MasterCard and Visa), ATM networks such as PULSE, NYCE or STAR, or the National Automated Clearing House Association (NACHA) Rules. Also remember to pay attention to the specific 'platform rules' such as developer rules for Apple, Google Play, Facebook or Twitter.

Will you 'own the customer' and be their primary point of contact?

The more data you collect, and the more hands-on you are in moving

money, the more legal rules apply. If users will upload funds to your mobile payments system via their choice of funding mechanisms for payment or future use (think PayPal here), then you will have Payment Card Industry Data Security Standards (PCI-DSS) obligations for card data, you will have to abide by NACHA rules for ACH authorisations (and revocations) and will have to connect to all of the payment rail networks via financial institutions (FIs), payment gateways, etc. The more control you have over the customer, the more you must be involved in dispute resolution under various association rules.

If you will be helping customers moving money from their accounts and funding sources to your company's accounts for transmission to third parties, then you are arguably engaging in money transmission, and if such funds will be sent abroad, you are engaging in foreign remittance.

And the analysis gets even more complicated for use of virtual currencies and sale of virtual goods, such as virtual currency funded by real money, earned by real-world actions, or awarded as part of contests, giveaways or sweepstakes. And if you can cash the virtual currency back out for real-world currency, that can also trigger money transmission laws.

What particular laws and legal issues should m-payments start-ups be aware of?

The current landscape of payment laws in the US is fragmented. Laws and rules governing credit card, debit card, ACH and wire transfers all developed independent of each other, with different consumer protections, disclosure requirements, and error resolution provisions. A variety of federal and state laws can apply to mobile payments apps and services. State laws can be triggered even where there is no physical presence or nexus of activity in the state.

The current landscape of payment laws in the US is fragmented. Laws and rules governing credit card, debit card, ACH and wire transfers all developed independent of each other, with different consumer protections, disclosure requirements, and error resolution provisions.

Many different laws can apply, including the following:

Payments-related laws

Electronic Funds Transfer Act/Regulation E: The Electronic Funds Transfer Act (EFTA) establishes the basic framework for the rights, liabilities, and responsibilities of consumers who use 'electronic funds transfer' (EFT) services. The primary objective of the law is consumer rights and consumer protection for individuals engaged in EFTs. The implementing regulation is the Federal Reserve Board's Regulation E. Under Regulation E, a mobile device used to initiate an electronic funds transfer from a consumer account is an 'access device,' and the issuer of the device or entity where the account resides is subject to Regulation E. Regulation E requires initial disclosures, periodic statements, and investigation and error resolution requirements. A Regulation E analysis of your mobile payments product is crucial because if it applies it will drive disclosures and error resolution procedures.

Truth-In-Lending Act/Regulation Z: TILA works to assure meaningful disclosure of credit terms to consumers so they can compare products, avoid uninformed use of credit, and be protected against inaccurate and unfair credit billing and credit card practices. Regulation Z, the rule enacting TILA, applies to consumer extensions of credit where credit is primarily for personal, family or household purposes. Regulation Z does not focus on the payment aspect that provides substantially immediate payment to the seller, but rather focuses on the credit aspect where the consumer commits to repay the entity extending credit at some time in the future.

Bank Secrecy Act/Anti-Money Laundering: If money or monetary value is being transmitted, or funds are held in mobile wallets or stored value products, currency is exchanged, bill payment occurs, etc., then federal Bank Secrecy Act and corresponding anti-money laundering requirements can apply. These requirements and obligations can include obligations to file certain reports with federal or state governmental agencies, or providing information to the mobile payments company's FI to facilitate such reporting. Your FI is required by law to gather certain information. To do the reporting, the mobile payments company may have to obtain and retain specific customer and transfer information. The mobile payments company may also have to register as a 'money services business' with FinCEN. The mobile payments company could have to maintain an appropriate anti-money laundering program in accordance with applicable law.

Money Transmittal Licensure: State and federal laws generally require licensure, and even licensing, to engage in activity that involves accepting funds and agreeing to transmit, transfer or pay funds to another party, except where the funds are used by the purchaser to directly pay for goods or services offered by the merchant itself. Money transmission licences can be very expensive and difficult to obtain. Where such licences are required, but have not been obtained and activity is occurring, civil and criminal penalties can apply.

Gift Card/Stored Value/Unclaimed Property Laws: Many 'pay now, buy later' payment models can trigger stored value/unclaimed property laws. If your mobile payments app or

service involves holding funds for future purchases, your company may have to comply with such laws, including filing required reports with state treasurers and comptrollers, giving notice to the property 'owners' and turning over the unclaimed funds/value to the appropriate states. Failing to comply with such unclaimed property laws can result in interest and penalties, which can sometimes exceed the initial amount remitted to the state. There are also laws prohibiting stored value funds from expiring and service fees being charged against the funds. The federal CARD Act of 2009 provides that the minimum expiration date on most types of gift cards (in any form) is five years, and prohibits most types of fees until at least 13 months after the gift card has been unused.

Other applicable laws and legal issues

Data privacy and security: This area is changing rapidly for mobile devices and activities regarding best practices for geo-location and mobile tracking (see FTC and California Attorney General recently issued best practices). The mobile payments company may also have to comply with the requirements of the federal Gramm-Leach-Bliley Act (GLBA) based on its activities. The sharing of information between third parties, even affiliates, for example, can trigger opt-out and opt-in requirements under GLBA and state laws. A mobile payments company must also follow its own published privacy policies or the FTC may come knocking. PCI-DSS card data requirements can also apply to certain mobile payments activities.

Intellectual property protection: Copyright, trademarks and especially patents must be top-of-mind for mobile payments companies. One high-profile patent infringement suit in the US involved multiple defendants including Starbucks, Expedia and Capital One. Mobile payment technologies and emerging business methods relating to mobile payments may be patentable subject matter, and companies may want to consider applying for patents as a defensive measure. In addition, many patents (some filed years ago) for mobile technology are being asserted against mobile payments in particular, which can lead to court battles even before product launch.

Child protection laws: Dealing with minors under 13 raises a whole host of issues, including the federal Children's Online Privacy Protection Act (COPPA). Some state laws addressing minors may apply until the minor is 16. Failure to comply can result in civil and criminal sanctions.

How can I build a brilliant m-payments app while dealing with all of this?

Understand that moving money is a regulated activity, and bake compliance and legal review into the process. Just like start-ups rely on corporate lawyers with start-up experience, mobile payments companies must call upon financial services/payments regulatory lawyers to vet the mobile payment product or service and facilitate compliance. While daunting, it is doable. Your mobile payments company is going head-to-head with many others in an incredibly competitive space. Don't get red-carded and thrown out of the game by failing to address the legal and compliance issues from the start.

Erin Fonté Shareholder and Payments Lawyer
Cox Smith Matthews
efonte@coxsmith.com
Twitter:@PaymentsLawyer

1. Source: John Stewart and Jim Daly, 'The Coming Shakeout in Mobile Payments,' Digital Transactions, Vol. 10, No. 1, Jan. 2013 at 28.
2. Source: IDC Financial Insights, 'Technology Selection: Worldwide Mobile Payments 2012-2017 Forecast' (Doc #FIN237814), available at: http://www.idc-fi.com/getdoc.jsp?containerId=FIN237814