Regulatory Report

for Payment Processors

TROUTMAN SANDERS

FROM THE REGULATORY AND ENFORCEMENT PRACTICE • SEPTEMBER 2016

CONTENTS

FEATURED ARTICLE

Getting Your Legal House In Order: Key Considerations For Selling Your Payment Processing Business

By Tyler Dempsey and Cot Eversole

Current mergers and acquisitions (M&A) activity in the payment processing and broader FinTech sectors is robust. Private equity sponsors and other financial investors are often attracted to payment processing companies with recurring cash flow streams and relatively low overhead. Strategic buyers in this industry are usually interested in acquiring new customer relationships and complementary product solutions.

Given the level of M&A interest in payment processing businesses from both financial and strategic players, business owners may be tempted to "strike while the iron is hot" and rush to put their companies on the market. While an extended company sale process can be a negative distraction to the business, most business owners understand that execution and completion of a successful project requires extensive preparation. In the case of the sale of a business, that preparation certainly includes items like ensuring that reliable financial statements are available, understanding the range of valuations for companies in the same or similar niche and assembling a team of experienced financial, legal and tax advisors.

One area that sometimes receives less focus in the context of a preparing a company for sale or investment is a review and analysis of the company's existing legal documents and framework. Often, parties will simply wait to receive a legal due diligence request list from a potential buyer or investor and then populate a "data room" with responses and react to any issues or questions that arise. An alternative suggested approach is for the company and its advisors to take a proactive role with legal due diligence. This proactive approach may result in resolving legal issues before they are raised as problems or concerns by a potential buyer or investor. At a minimum, the company and its advisors should be better-versed on the relevant issues and able to craft a proposed solution (as opposed to being caught by surprise). In addition to streamlining the due diligence process, an advanced review of a company's legal documentation is advisable in order to assist advisors in developing a proper transaction structure and in executing a successful transaction.

Typical areas for getting your "legal house in order" in advance of a company sale or investment transaction are described below. While some of these considerations are

generally applicable to all businesses, they are particularly relevant to most payment processing companies.

Capital Structure

A proper understanding of the company's current ownership structure is critical in the context of a potential sale or investment transaction. Clear documentation relating to the relative rights and obligations of the various equityholders is essential. The terms of the company's "distribution waterfall" and the presence (or absence) of drag-along provisions and similar terms can have a material impact on whether a certain transaction is attractive to the various stakeholders or if it is even feasible. Similarly, because many payment processing companies offer equity incentives to their employees, it is important that the equity incentive awards are appropriately documented and that the terms of the underlying plan (including applicable vesting provisions) are clear and understood from the outset.

The structure of a sale or investment transaction will often be dependent on the company's tax status (i.e., C-corporation, S-corporation or partnership). Accordingly, it is important that the parties' assumptions about the company's tax status are confirmed as early as practicable. In particular, S-corporation status requires compliance with highly technical tax rules. Some inadvertent violations of these S-corporation rules can be cured if there is ample time.

Employment Matters

The acquisition of top management and employee talent is often one of the key reasons that a potential purchaser or investor pursues a payment processing company. As a result, employee relations and related documentation will be a key focus of any due diligence investigation.

Some payment processing companies are able to generate significant revenue with relatively lean employee staffing requirements. But the failure of a business to comply with the myriad of applicable employment laws can still result in material risk and exposure. Particularly since a small-to-midsize payment processing business may not have strictly defined roles for all employees, companies should consider conducting a self-assessment with respect to the exempt vs. non-exempt classification under the Fair Labor Standards Act. Similarly, a fast-growing payment processing business may have elected to utilize independent contractors for the performance of certain services or functions. However, these types of determinations are now under greater scrutiny, and a misclassification can result in liability for failure to withhold income and employment taxes, as well as a claim by the service provider (even if the service provider initially agreed with – or even requested – the independent contractor classification).

A potential buyer or investor will be keenly interested in whether the company's employees are bound by appropriate agreements that protect the company's confidential and proprietary information and its relationships with customers, employees and key business partners. The company's counsel should review these business protection agreements to confirm both that they adequately address the company's needs and that they are enforceable under applicable state law. If material deficiencies or omissions are identified, the company should strongly consider putting appropriate agreements in place with key employees at the outset of any sale or investment process.

Legal Proceedings and Investigations

Any company considering a sale or investment transaction should gather summary information for all pending, threatened or recently settled litigation, arbitration and regulatory proceedings. To the extent outstanding claims can be settled or resolved in an expedient and commercially reasonable manner, the company should consider doing so; otherwise, material outstanding litigation can be a distraction during due diligence (and potentially adversely affect valuation). If quick resolution is not a feasible option, then the company and its advisors should develop a plan to share the relevant information with the potential buyer or investor while preserving the attorney-client privilege and similar protections.

Material Business Contracts

Contracts with customers, vendors and key partners constitute the "DNA" of the typical payment processing business. It is critical that the company and its advisors have a firm grasp of the material terms and conditions of these contracts as early as possible in a potential sale or investment process. This is particularly important due to the interrelated nature of many of these contracts, as well as the fact that it is not uncommon in the payment processing industry for a company's key vendor or partner to also be an actual or potential competitor. These factors will almost certainly be highlighted and stress-tested in a due diligence investigation in connection with a potential sale or investment transaction.

In addition to the key business and economic issues (e.g., initial and renewal terms, pricing, etc.), attention should be paid to the following contractual provisions in connection with any preliminary evaluation of a payment processing business:

- Anti-Assignment/Change of Control Provisions – the exact wording of these provisions may require the consent or waiver of the other party to the contract in connection with a potential sale or investment transaction.

- Exclusivity Provisions – these provisions may dictate whether one party is the exclusive provider or marketer of specified services or solutions.

- Non-Solicitation or Non-Circumvention Provisions – these provisions may restrict one party from soliciting or contacting certain customers, employees and other third parties under certain conditions for a specific period of time.

- "Most-favored nation" Provisions – these provisions may require a provider or other party to give a customer or other partner the best terms it makes available to any other customer or similar partner.

The summaries above are very high-level in nature. Each particular contract provision needs to be carefully analyzed in the light of the specific facts and circumstances. A contract that was executed at an early stage of a payment processing company's life cycle may have unintended consequences if assumed by a larger and more diversified player in the industry.

Intellectual Property Matters

Together with contractual relationships and management talent, intellectual property rights typically represent one of the key "assets" that a potential purchaser or investor is buying in a payment processing business. The first step in this regard for a company considering a sale or investment transaction is to summarize the company's intellectual property portfolio (patents, trademarks, designs, copyrights, trade secrets, databases, software or other types of intellectual property) and be clear about what items are owned versus licensed. For customized licensed software, careful review of the applicable license agreements is recommended in a manner similar to the "Material Business Contracts" section above.

If proprietary software is material to the current or proposed conduct of the company's business, then the company and its advisors should consider preemptively conducting the level of due diligence that a typical investor or buyer would: namely, identifying all individuals involved in the development of the software and verifying that appropriate assignment language in favor of the company is in place. If there are any "gaps" in this chain of title exercise, it is typically advisable to try to remedy the issue at an early stage of a sale or investment process. Lastly, the company and its advisors should identify and understand the extent to which "open source" software is utilized by the company in connection with its intellectual property development efforts. Under certain circumstances, using open source software without the proper safeguards could require unexpected disclosure of proprietary source code and exposure to other undesirable risks.

Licenses and Permits

Payment processing organizations are subject to a myriad of complex (and ever-evolving) regulations at the federal, state and association levels. The company's exact regulatory framework and required licenses and permits will depend on the particulars of the company's business model. Qualified regulatory counsel should be consulted relatively early in any potential sale or investment transaction process in order to assess the level of regulatory advice that the company has received to date and to plan for the expected inquires from a potential purchaser or investor.

• • •

As is probably apparent from the above, an investment of time and resources will be required in order for a payment processing company to get its "legal house in order" in a connection with a potential sale or investment transaction. Many companies avoid taking a proactive approach with respect to legal due diligence in order to save expenses. However, this decision will often prove to be "penny wise and pound foolish." When these types of issues arise during the legal due diligence conducted by the advisors of a potential buyer or investor, there is usually a delay in the timing of the transaction and the ultimate outcome is typically an adverse impact on the company's valuation or the assumption of increased exposure (through indemnification or otherwise) by the seller owners of the business. Conversely, with some preliminary homework at the beginning of a sale or investment process, many of the legal issues of this nature can be dealt with ahead of time or at least be the subject of a thoughtful approach and plan. Any payment processing company that is contemplating a sale or investment transaction should consider being proactive with respect to the legal due diligence process and working with its counsel to review and analyze the areas described above that are material to its business.

Tyler Dempsey is a partner at Troutman Sanders LLP where he is a member of the Corporate, and Payments and Other Financial Technology practices.
tyler.dempsey@troutmansanders.com • 404.885.3764

Cot Eversole is an associate at Troutman Sanders LLP where he is a member of the Corporate practice.
cot.eversole@troutmansanders.com • 404.885.3439

New York AG Announces Data Breach Settlement with EZcontactsUSA

By Ashley L. Taylor, Jr., Mark C. Mao, Ronald I. Raether, Jr. And C. Reade Jacob, Jr.

On August 5, the New York Attorney General announced a settlement with Provision Supply, LLC, d/b/a EZcontactsUSA.com over a data breach resulting in the potential exposure of over 25,000 credit card numbers and other cardholder data. Provision Supply, the operator of EZContactsUSA.com, a Brooklyn-based e-tailer that sells contact lenses and eyewear, agreed to pay $100,000 in penalties and to shore up its data security practices.

According to the New York A.G.'s press release, EZContactsUSA.com's website experienced a third-party breach in August 2014. The company became aware of the breach as much as a year later when its merchant bank informed it that fraudulent charges were being posted to customers' credit card accounts.

The A.G. found that EZContactsUSA.com failed to provide notice to its customers or law enforcement officials about the breach, in violation of New York's data breach notification law. General Business Law § 899-aa requires that notice be provided to affected individuals and various government agencies in the most expedient timeframe possible and without unreasonable delay.

The AG's press release placed great emphasis on EZcontactsUSA's claims that their website was "100% safe and secure" when, in reality, their website had numerous vulnerabilities. Executive Law § 63(12) and General Business Law §§ 349 and 350 prohibit misrepresenting the safety and security of a website.

The settlement requires EZcontactsUSA.com to conduct thorough and expeditious investigations of any future data security breaches, to provide prompt notice of data security breaches to affected New York residents and to New York law enforcement agencies, to maintain reasonable security policies and procedures designed to protect the personal information of consumers in accordance with New York State General Business laws, and to remediate the many security vulnerabilities contained in its website. EZcontactsUSA.com will also be required to train employees with the most up-to-date data security practices.

Washington AG Sues Comcast for Alleged Deceptive Practices, Seeks Over $100 Million

By Lillian Macartney, Stephen C. Piepgrass And Steve D. Rosenthal

The Washington Attorney General has filed a lawsuit against internet and cable company Comcast, alleging more than 1.8 million violations of the Washington state Consumer Protection Act and seeks over $100 million in penalties as well as injunctive relief. The Washington Attorney General's Office says that the lawsuit is the "first of its kind in the nation," noting that many of the alleged deceptive practices involve nationwide programs.

The claims stem from the company's Service Protection Plan, the fees it charges customers for service calls, and its practices of running credit checks on certain customers. The suit alleges that Comcast "grossly misrepresented" the Service Protection Plan, which is an optional add-on that customers may purchase to allow them to avoid certain service fees. The Attorney General claims that while Comcast advertised that the Plan provided comprehensive coverage, the Plan in fact only applies to a narrow scope of repairs. For instance, while advertising that the Plan covers "inside wiring," the Plan does not cover wiring inside the walls of a consumer's home. Similarly, Comcast advertises coverage of certain problems that are already covered for free by the Comcast Customer Guarantee. The complaint notes that over 500,000 Washington residents subscribed to the Plan in the past five years, and have paid at least $73 million to Comcast during that time.

The complaint further alleges that customers were improperly charged for service fees that should have been covered for free by the Comcast Customer Guarantee. The complaint notes that until June 2015, Comcast provided its technicians with a service code that allowed them "to add service charges to a normally not charged fix code."

Finally, the complaint accuses Comcast of improperly charging deposits or running credit checks on more than 6,000 customers.

Attorney General Bob Ferguson stated in a press release, "This case is a classic example of a big corporation deceiving its customers for financial gain."

Among other things, the lawsuit highlights the importance of having meaningful communication with the Attorney General's Office. The Washington A.G. noted in its press release that it brought up concerns with Comcast over a year before filing the action, but stated that the company did not make any internal changes until litigation was imminent.

Members of Troutman Sanders' Regulatory Compliance and Investigations Group have experience providing advice and assisting businesses engaged with attorney general investigations.

Payment Processor Group Files Amicus Brief in CFPB v. Intercept Case

By C. Reade Jacob, Jr., Ashley L. Taylor, Jr. And Keith J. Barnett

On August 15, the Third Party Payment Processors Association ("TPPPA"), a national, not-for-profit organization of payment processors, payroll processors, and banks, this week filed a brief, amicus curiae, in support of the defendants' motion to dismiss in the Consumer Financial Protection Bureau's lawsuit against Intercept. The TPPPA filed the amicus brief in the United States District Court for the District of North Dakota (Case No. 3:16-cv-00144-ARS).

According to a press release issued by the TPPPA, the group filed the amicus brief in light of the CFPB's position that certain conduct should be deemed "unfair" under the Consumer Financial Protection Act without alleging a violation of a substantive federal law or industry rule. The TPPPA believes that this position will adversely affect the due process rights of all third party payment processors and others in the payments industry if the lawsuit is not dismissed.

The TPPPA's amicus brief noted that unlike banks, which have clearly identified regulators, no federal regulator directly supervises non-bank payment processors, and there is not a body of federal law that is particular to payment processors. The conduct of non-bank payment processors is governed by the NACHA Operating Rules, the well-established industry rules for ACH payments.

The amicus brief argues that the CFPB's complaint against Intercept failed to provide substantive proof that Intercept violated the NACHA Rules that were in place at the time the alleged violations occurred. In fact, the complaint never alleged that Intercept or its banks had ever received a rules violation from NACHA as a result of Intercept's actions. Therefore, TPPPA urged the Court to reject the CFPB's allegations that the actions of Intercept are unfair under the CFPA.

"The ACH Network combines the mutual benefits of low cost electronic payment processing to business with the protection of consumers afforded them by Regulation E," said Marsha Jones, president of the Third Party Payment Processors Association. "In fact, the warranties of the bank originating the payments extend beyond the typical Regulation E 60-day timeframes, to ensure that the consumer is made whole from any unauthorized ACH entries to their account, including any bank fees like overdraft fees, that may have resulted because of the unauthorized entry. This makes the ACH Network arguably the most consumer friendly payment system available in the United States."

The press release notes that the payments industry is evolving very quickly, with payments shifting from traditional in-person payments to global payments over the Internet, both of which make "Know Your Customer" more and more difficult. At the same time, the speed of payments is increasing as evidenced by the ACH Network moving into Same Day ACH payments next month.

"Compliance with federal regulations related to electronic payments is evolving very quickly to keep pace with the ever-

changing payments landscape," according to Keith J. Barnett, an attorney with Troutman Sanders who filed the amicus brief on behalf of the TPPPA. "There are consumer protection regulations being amended, along with a relatively new regulator in the CFPB, and new rules on Customer Due Diligence related to beneficial owners, as well as the ongoing concerns with Anti-Money Laundering. And this is just at the federal level. Consider that 50 states' laws in a global Internet payments ecosystem make all of this exponentially more complex and confusing for businesses."

"We acknowledge the need to evolve the legal and regulatory framework around electronic payment processing and are committed to be leaders in this effort, in part by continually improving the TPPPA's Compliance Management System," said Jones. "However, we cannot stand idly by and allow payment processors and banks to be held accountable for laws, rules and regulations that did not exist when the alleged actions occurred. This is why we felt compelled to provide an industry perspective to the court in the form of an amicus brief."

South Carolina Governor Signs Money Transmitter Law

By Keith J. Barnett, Ashley L. Taylor, Jr. And C. Reade Jacob, Jr.

On June 9, 2016, South Carolina Governor Nikki Haley signed into law the South Carolina Anti-Money Laundering Act. The South Carolina AML Act, among other requirements, imposes a license requirement for persons and entities engaged in money transmission in the state. South Carolina is now the 49th state to implement a law regulating money transmitters – leaving only Montana as the only state without a money transmitter law.

Under the new South Carolina law, which will take effect in one year, a license is required for persons that "engage in the business of money transmission or advertise, solicit, or hold himself out as providing money transmission. " The law defines money transmission to include "selling or issuing payment instruments, stored value, or receiving money or monetary value for transmission."

Importantly, the law provides a number of exclusions from the money transmission rules. For example, federal and state banks are excluded from the law so long as they do not engage in "money transmission" through non-bank agents. Also excluded from the law are operators of a payment system to the extent the system provides processing and clearing or settlement services between or among persons excluded under the law in connection with wire transfers, credit card transactions, debit card transactions, stored-value transactions, ACH transfers and similar funds transfers.

The law also contains a potential exception for persons already licensed as a money transmitter in at least one other state, so long as (1) the person obtains approval of the South Carolina Securities Commissioner; (2) the state in which the person or entity is licensed as a money transmitter has enacted the Uniform Money Services Act or the commissioner determines that the money transmission laws of that state are substantially similar to those proposed in the bill; and (3) the person or entity submits an application for approval to operate without a license in the state along with a non-refundable $1,000 fee and a certification of license history in the other state.

The Act imposes various financial obligations on applicants and licensees. An applicant is required to submit a nonrefundable $1,500 application fee and a $750 license fee, which will be returned if the application is denied. An application must also be accompanied by "a surety bond, letter of credit, or other similar security acceptable to the commissioner" of $50,000 plus $10,000 for each location, not exceeding a total of $250,000. However, the commissioner may increase the amount of security required to a maximum of $1,000,000 "if the financial condition of a licensee so requires, as evidenced by reduction of net worth, financial losses, or other relevant criteria."

Licensees are required to pay an annual renewal fee of $750 and maintain a net worth of at least $250,000 and comply with a permissible investment requirement. Additionally, the new law will subject licensees to various examination and reporting obligations.

The South Carolina Securities Commissioner is able to assess a civil penalty of $1,000 per day for each day a violation of the

act is outstanding, plus costs, expenses, and attorney fees. The new law also imposes felony liability for certain knowing and intentional acts.

The law takes effect one year after approval of the governor or upon the publication in the State Register of final regulations implementing the law, whichever occurs later.

Minnesota AG Settles Lawsuit with Online Payday Lender

By Keith J. Barnett

On August 18, 2016, the Minnesota Attorney General announced that it had settled a lawsuit against online money lender Cash Call, Inc. The announcement is here. The State of Minnesota alleged that Cash Call violated Minnesota's usury, lending, and licensure laws by entering into an arrangement in which a company affiliated with a Native American tribe would loan money to Minnesota citizens at interest rates as high as 342 percent and then transfer those loans to Cash Call for servicing and collection. The 342 percent exceeded the Minnesota interest rate limits.

Under the terms of the settlement, all outstanding loans to Minnesota residents have been forgiven. If Cash Call sold a loan to a third party, the settlement requires CashCall to send a letter to the third party directing the third party to forgive the loan. In addition, CashCall must send a letter to the consumer reporting agencies to which it reported directing the consumer reporting agencies to remove any reporting about the loan from consumers' credit report. CashCall also made a $4.5 million restitution payment to Minnesota.

Minnesota's settlement with CashCall is a part of a growing trend of states executing settlement agreements with lenders arising out of the lenders' alleged violations of state licensing and usury laws. In fact, CashCall recently executed similar settlements with the States of Arkansas and Michigan. These cases are particularly important to payment processors, as states have filed lawsuits or executed settlement agreements with lenders and processors arising out of allegations that the lenders violated a state's usury laws.

CONTACTS

Ashley L. Taylor, Jr.
804.697.1286
ashley.taylor@
troutmansanders.com

Keith J. Barnett
404.885.3423
keith.barnett@
troutmansanders.com

The Troutman Sanders' **Consumer Financial Services Law Monitor** blog offers timely updates regarding the financial services industry to inform you of recent changes in the law, upcoming regulatory deadlines and significant judicial opinions that may impact your business. Visit the blog for current updates at www.cfslawmonitor.com.