WHAT DEBT SETTLEMENT COMPANIES NEED TO KNOW WHEN WORKING WITH THIRD PARTY PAYMENT PROCESSORS

January, 2025

This whitepaper is authored by Clark Hill's Financial Services and Regulatory Compliance Group. The paper provides an objective legal and regulatory overview of the payment processing landscape in order for debt settlement companies to make informed decisions about the partners they choose to work with. RAM Payment, LLC ("Reliant") commissioned Clark Hill to write the whitepaper as a resource for industry participants. The opinions and conclusions expressed in this whitepaper are not endorsed or approved by Reliant and are solely the opinions and conclusions of Clark Hill based upon the law and regulations cited herein. This whitepaper does not take into account the factual circumstances of any individual or entity and should not be relied upon as legal advice for any matter. This whitepaper does not establish an attorney client relationship between Clark Hill PLC and any individual or entity. If you have a legal issue that relates to the topics of this whitepaper, you should contact an attorney for assistance in your matter.

Contents

EXECUTIVE SUMMARY

For a debt settlement company (DSC), payment processors play an essential role in facilitating business operations. Because a DSC is typically classified as a "high-risk" business[i], they often face limitations in obtaining merchant accounts through many sponsoring banks.[ii] As a result, a DSC typically engages a third-party payment processor to hold and manage accounts and handle financial transactions for both the DSC and their consumer (debtor) customers. Under the Federal Trade Commission's (FTC) Telemarketing Sales Rule discussed in detail below, a DSC may only request or require a customer to place funds in an account to be used for the DSC's fees and for payments to creditors or debt collectors as long as certain strict requirements are met. These requirements are specifically designed to ensure an independent, arms-length relationship between the DSC and the payment processor in order to avoid conflicts of interest and to protect the consumer's funds.

Third-party payment processor arrangements introduce significant risks for the DSC and the payment processor. These risks include but are not limited to potential liability for the DSC arising from the payment processor's noncompliance with the law and regulatory compliance standards; potential liability to the payment processor for a DSC's noncompliance with the law and regulatory compliance standards, and possible class action exposure for both the DSC and the payment processor. These arrangements can also result in significant risk to consumers in the event of a potential exposure of sensitive consumer data.

A DSC is therefore responsible for managing risks associated with their relationship with a third-party payment processor. This includes adhering to the Third-Party Risk Management (TPRM) guidance issued by prudential regulatory bodies such as the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC), commonly known as the "the Interagency Guidance"[iii]. Prudential regulators have an interest in payment processors in the debt settlement space because they set up accounts for the consumer at a bank and their activities directly touch consumers' deposit accounts and funds. Additionally, the Consumer Financial Protection Bureau's (CFPB) guidance on service providers[iv] as well as the CFPB's jurisdiction over the law governing electronic payments reinforces this requirement of oversight by DSCs.

As a non-bank, a DSC may have the same responsibilities as traditional financial institutions and banks for the oversight of the service providers they hire to assist in the delivery of the products and services offered to consumers. Therefore, it is imperative for a DSC to fully understand the laws and regulations applicable to the DSC and their payment processors and to ensure those payment processors are complying with the law, in addition to a DSC's own regulatory compliance with the law.

This whitepaper outlines and provides insight into the requirements governing oversight over third party payment processors; explores the various laws and regulations that are integral for a DSC when developing a robust and well-executed third party risk management program with its payment processing partner; provides an overview of federal and state enforcement actions when those laws and regulations are not followed by either a DSC or a payment processor; and finally, outlines key contractual provisions taken directly from the Interagency Guidance that should be considered by a DSC when entering into a business relationship with a payment processor.

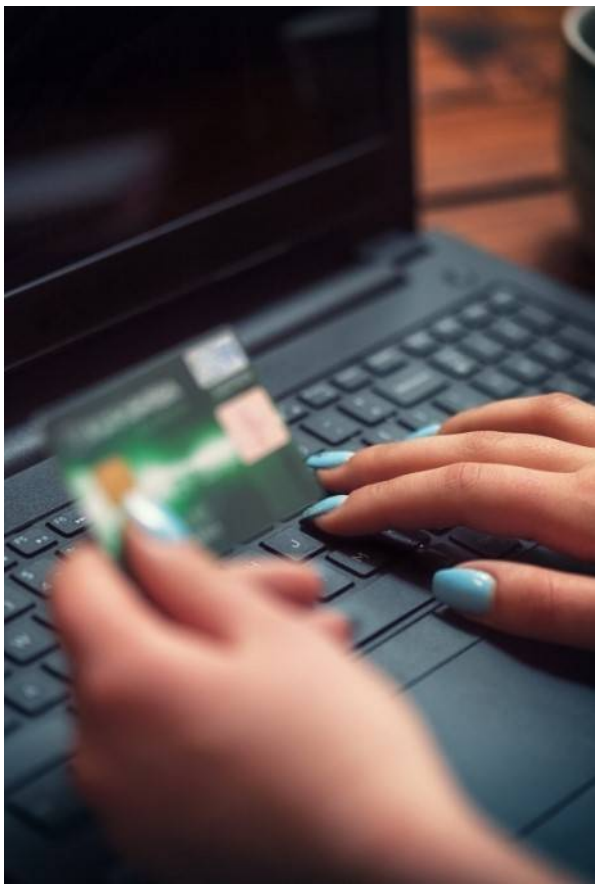
INTRODUCTION

Over the past two decades, the payment processing landscape has undergone significant innovation, evolving from a cash-dependent model to one where credit and debit card payments and electronic funds transfer payments are a standard expectation for consumers and businesses alike. These developments have resulted in higher risks for both payment processors and their clients. Given this landscape, a DSC must understand and incorporate rigorous regulatory oversight of the payment processor with which they choose to work. Understanding the regulatory requirements and expectations will enable a DSC to comprehend the scope of and to satisfy their required oversight of payment processors.

THIRD-PARTY RISK MANAGEMENT (TPRM)

General Overview by Regulators

Prudential regulators (OCC, FDIC and the FRB) as well as the CFPB and the Federal Trade Commission (FTC) mandate that covered entities manage and oversee their third-party service providers to ensure adherence to all applicable consumer financial protection laws and the security of customer information. The prudential regulators have collectively provided Interagency Guidance on third-party risk management (TPRM),[v] that is relevant not only for banks but instructive for all financial institutions, including non-banks like DSCs, that engage third parties in their operations. The Inter-Agency Guidance reaffirms that the use of third parties does not diminish the responsibility to meet regulatory requirements to the same extent that the activities were performed by the financial institution or non-bank in-house.[vi] In 2016, the CFPB re-issued similar guidance regarding the oversight of service providers (third parties) who provide financial products and services to non-banks.[vii] Like prudential regulators, the CFPB also reaffirms that non-banks should "take steps to ensure that their business arrangements with service providers do not present unwarranted risks to consumers." [viii] The CFPB notes in its guidance that "while due diligence does not provide a shield against liability for actions by the service provider, it could help reduce the risk that the service provider will commit violations for which the supervised bank or nonbank may be liable". Therefore, it is essential for a DSC to develop and implement a TPRM program when engaging a payment processor in order to mitigate potential regulatory and compliance risks which could result in liability to the DSC. Finally, the FTC's Standards for Safeguarding Customer Information [ix] (known as the Safeguards Rule) requires that entities covered by the Rule maintain safeguards to protect the security of customer information.[x] The Safeguards Rule took effect in 2003 and has been amended twice since then: in 2021 to provide more concrete guidance for businesses regarding core data security principles that all covered entities must implement, and in 2023 to require covered entities to report certain data breaches and security incidents.



Elements of TPRM Program

Both Interagency Guidance and the CFPB guidance, as well as the FTC's Safeguards Rule, outline important steps incumbent upon banks and non-banks, like DSCs, for the oversight of their service providers like payment processors. These steps should include, but are not limited to:

- Conducting thorough due diligence to verify that the service provider understands and is capable of complying with Federal consumer financial laws;
- Requesting and reviewing the service provider's policies, procedures, internal controls, and training materials to ensure that the service provider conducts appropriate training and oversight of employees or agents that have consumer contracts and compliance responsibilities;
- Including in the contract with the service provider clear expectations about compliance, as well as appropriate and enforceable consequences for violating any compliance-related responsibilities, including engaging in unfair, deceptive, or abusive acts or practices;
- Establishing internal controls and on-going monitoring to determine whether the service provider is complying with Federal consumer financial laws; and
- Taking prompt action to address fully any problems identified through the monitoring process, including terminating the relationship where appropriate.

The OCC, as part of the Interagency Guidance, highlights additional risk areas for entities, liked a DSC, to consider and adopt when developing a TPRM [xi] Program:

Planning and Risk Assessment. An evaluation of the extent of risk-management resources and practices for effective oversight of the proposed third-party relationship throughout a third-party relationship life cycle;

Due Diligence. The process of assessing, prior to entering into the third-party relationship, the third party's ability to perform the requested activity as expected, to adhere to policies, to comply with all applicable laws and regulations, and to conduct the activity in a safe and sound manner.

Contract Negotiation. The negotiation of contract provisions with the third party that will facilitate effective risk management and oversight which should specifically outline the expectations and obligations of both parties. (See, Contract Negotiation Section)

Ongoing Monitoring. Ongoing monitoring of the third party's performance will ensure the third party is performing as required for the duration of the contract. This includes (1) confirming the quality and sustainability of a third party's controls and ability to meet contractual obligations; (2) escalating significant issues or concerns, such as material or repeat audit findings, consumer complaints, deterioration in financial condition, security breaches, data loss, service interruptions, compliance lapses, or other indicators of increased risk; and (3) responding to such significant issues or concerns when identified.

Termination. The impact of a potential termination should be considered during the planning stage of the life cycle as it may help to mitigate costs and disruptions caused by termination, particularly for higher-risk activities.

Governance. Governance practices throughout the third-party relationship life cycle: oversight and accountability, independent reviews, and documentation and reporting, must be considered.

Oversight and Accountability. A board of directors has ultimate responsibility for providing oversight for third-party risk management and holding management accountable. This includes developing and implementing third-party risk management

policies, procedures, and practices, commensurate with the organization's risk appetite and level of risk and complexity of its third-party relationships.

Independent Review. There must be periodic and independent reviews to assess the adequacy of its third-party risk management processes. The results of an independent review determine whether and how to adjust its third-party risk management process, including its policies, reporting, resources, expertise, and controls.

Documentation and Reporting. While oversight activities may vary among organizations depending on the risk and complexity of their third-party relationships, these activities must be well documented.

If during the planning and assessment stages of a TPRM program, a DSC cannot address any one of the elements noted above, then the DSC should carefully consider whether the relationship is appropriate under the circumstances and what other options exist. For example, if a DSC cannot obtain desired due diligence information from the third-party, the DSC should consider alternative information, controls, or monitoring, as well as consider another payment processing partner.

The remainder of this white paper will explore the various laws and regulations that are integral for a DSC when developing a robust and well-executed TPRM program with its payment processor; provides an overview of federal and state enforcement actions when those laws and regulations are not followed by either a DSC or a payment processor; and finally, and outlines key contractual provisions that should be considered by the DSC when entering into a business relationship with a payment processor.

DIFFERENCES BETWEEN PAYMENT PROCESSORS AND MONEY TRANSMITTERS

What is a Payment Processor?

A payment processor is a company or service that facilitates electronic transactions between a business and its customers, enabling businesses to accept electronic payments. [xii] Acting as an intermediary, the payment processor, in most instances, connects the customer's bank with the merchant's (the business's) bank, ensuring that transactions are authorized, processed, and completed securely. Payment processors handle a wide array of traditional, core banking payment types, including credit card payments, debit card transactions, electronic funds transfer (EFT) payments, automated clearinghouse (ACH) transactions, digital wallets, and in-person transactions through point-of-sale (POS)

systems. The term "payment processor" does not have a statutory definition under federal law or in state regulations. Instead, it is a generally understood term used throughout industry practice and regulatory guidance.

What is a Money Transmitter?

A money transmitter facilitates a broader range of financial services and money transfers, including person-to-person transfers, remittances, business payments, transmitting money by facsimile or other electronic communication, and making international transfers [xiii], as opposed to a payment processor that focuses primarily on core banking payment transactions between businesses and consumers. Due to the broader scope of services they provide and because of the higher risk nature of some of their payment activities, money transmitters are subject to more stringent regulatory requirements than payment processors. These include mandatory registration as a money service business with the Financial Crimes Enforcement Network (FinCEN)[xiv] and possible licensing in 48 states, except for Montana and Massachusetts.[xv] Money transmitter laws are principally designed to protect consumers and to regulate these entities to ensure compliance with Bank Secrecy Act (BSA) and anti-money laundering (AML) laws and regulations and Office of Foreign Assets Control (OFAC) requirements. These requirements apply broadly to organizations that handle or facilitate the movement of money on behalf of others, so there may be instances where, depending on what types of payments it processes, a payment processor could also be considered a money transmitter.

When Does a Payment Processor Become a Money Transmitter?

Whether a payment processor should be licensed as a money transmitter is determined under state law and FinCEN regulations based upon the activities engaged in by the payment processor. While there is no specific state licensing requirements for payment processors, many states require entities that are engaged in the business of money transmission to obtain a money transmitter license (MTL). Because a payment processor's activities could result in an entity being defined as a money transmitter, a DSC must fully understand whether their payment processor is also deemed a money transmitter that requires a license.

An organization is generally considered a money transmitter if it engages in activities such as:

- **Transferring funds between individuals or entities:** This includes sending or receiving payments on behalf of customers.
- **Facilitating stored value transactions:** Providing services like prepaid cards or digital wallets.
- **Accepting and holding funds for later disbursement:** Holding consumer funds for purposes such as settling debts or paying bills.

These common definitions are delineated in states that require a MTL.[xvi]

The determining factor underlying the money transmitter designation is the issue of control and whether the entity has control over the consumer's funds and is actively engaged in transferring or holding money for others. [xvii] Whether a person or entity is a money transmitter is a matter of facts and circumstances. FinCEN regulations outline the following activities engaged in by money transmitters:

> (A) Provides the delivery, communication, or network access services used by a money transmitter to support money transmission services;
>
> (B) Acts as a payment processor to facilitate the purchase of, or payment of a bill for, a good or service through a clearance and settlement system by agreement with the creditor or seller;
>
> (C) Operates a clearance and settlement system or otherwise acts as an intermediary

solely between BSA regulated institutions. This includes but is not limited to the Fedwire system, electronic funds transfer networks, certain registered clearing agencies regulated by the Securities and Exchange Commission ("SEC"), and derivatives clearing organizations, or other clearinghouse arrangements established by a financial agency or institution;

(D) Physically transports currency, other monetary instruments, other commercial paper, or other value that substitutes for currency as a person primarily engaged in such business, such as an armored car, from one person to the same person at another location or to an account belonging to the same person at a financial institution, provided that the person engaged in physical transportation has no more than a custodial interest in the currency, other monetary instruments, other commercial paper, or other value at any point during the transportation;

(E) Provides prepaid access; or

(F) Accepts and transmits funds only integral to the sale of goods or the provision of services, other than money transmission services, by the person who is accepting and transmitting the funds. [xviii]

Payment processors are **less** likely to be classified as money transmitters, as they typically act as intermediaries facilitating payment transactions without controlling the funds. Furthermore, with respect to DSCs, payment processors contract with the debt settlement companies directly and not through the underlying creditors of the DSC. Therefore, section (B) as noted above, would not be applicable to payment processors who work with DSCs.

However, a payment processor might be required to be licensed as a money transmitter if it:

- Accepts and holds funds for settlement over an extended period of time; and.
- Offers additional financial services, such as managing stored value or disbursing funds directly to third parties.

Example Scenario – MTL License Trigger

A payment processor debits consumer accounts and holds funds for several days before remitting them to a creditor or DSC. This activity could trigger money transmitter licensing requirements, as the processor is temporarily controlling consumer funds. Conversely, if the processor simply facilitates the immediate transfer of funds between the consumer and the creditor without holding funds, it would not require a MTL. [xix]

DSCs and payment processors should carefully analyze their business models and fund flow processes to determine if the activity involved results in the trigger of a MTL requirement. Noncompliance with state money transmitter laws can result in significant penalties and operational disruptions. Determining whether a payment processor qualifies as a money transmitter is crucial for DSCs. This ensures compliance with applicable regulations and safeguards against the risks of working with unlicensed entities, which can result in significant operational challenges, financial fines and penalties and negative legal repercussions.

RELEVANT STATUTES AND REGULATIONS WHICH GOVERN DSCs AND PAYMENT PROCESSORS

The Telemarketing Sales Rule (TSR) [xx] and Regulation E (Reg E) which implements the Electronic Funds Transfer Act (EFTA), are the most important regulations DSCs must consider not only for themselves in terms of compliance but also to ensure that their payment processor partners are in compliance as well.

The Telemarketing Sales Rule (TSR)

Overview

The Telemarketing Sales Rule (TSR) is an important regulation governing telemarketing practices within the United States. The Federal Trade Commission (FTC) has primary jurisdiction over the TSR to protect consumers from deceptive and abusive tactics[xxi] when they are being telemarketed. With certain exceptions, a DSC or any individual involved in telemarketing must comply with the TSR. DSCs are subject to TSR requirements when (i) initiating or receiving calls from consumers, or when (ii) offering, arranging, or providing their services in exchange for fees, which includes services aimed at reducing the balance, interest rate, or fees owed by the consumer to the consumer's creditor(s).

There are important definitions to the TSR:

- ***"Telemarketing"*** is defined as "a plan, program, or campaign . . . to induce the purchase of goods or services or a charitable contribution" involving more than one interstate phone call.[xxii]
- ***Telemarketers"*** are defined as any person who, in connection with telemarketing, initiates or receives telephone calls to or from a customer or donor. [xxiii]
- **"Sellers"** are defined as any person who, in connection with a telemarketing transaction, provides, offers to provide, or arranges for others to provide goods or services to the customer in exchange for consideration. [xxiv]
- **Debt settlement** is referred to as ***"debt relief services"*** under the TSR and is defined as any program or service represented—explicitly or implicitly—as renegotiating, settling, or altering the terms of debt between a person (i.e. an individual consumer) and an unsecured creditor or a debt collector. [xxv]

Prohibited Practices

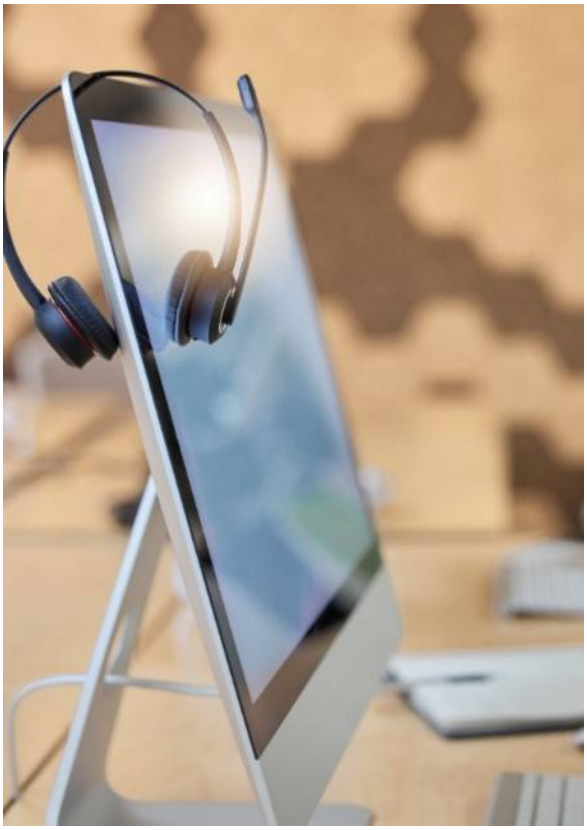
The TSR outlines prohibited deceptive and abusive practices relative to telemarketing.[xxvi] Several key areas include the ban on misrepresentations, the limitation on payment structures (such as the prohibition on advance fees for debt relief services), and the requirement for clear disclosures regarding services provided. In addition, the TSR imposes substantial recordkeeping requirements on DSCs. Failure to comply with these requirements will not only result in a violation of the TSR but will make it difficult for a DSC to support and prove that it is not engaging in those prohibited practices.

In order to ensure the independence between the DSC and the payment processor and to protect the consumer's funds pursuant to 16 CFR §310.4(a)(5)(ii), the TSR also mandates strict requirements for handling and managing consumer accounts if the DSC requests or requires the consumer to place funds in a dedicated account to be used to pay the consumer's creditors, and when appropriate, pay for the fees owed to the DSC. A DSC may request or require that a consumer's funds be held in a dedicated account as long as a litany of safeguards are implemented to protect consumer funds as well as maintain the arm's length and conflict free relationship between the DSC and its payment processor: A consumer's funds may only be held in a dedicated account as long as all of the following requirements are met:

- The consumer's funds are held in an account at an insured financial institution;
- The consumer owns the funds (including any interest accrued) and is paid any accrued interest on the account;
- The DSC does not own or control the payment processor administering the account or have any affiliation with it;
- The DSC doesn't split fees with, or accept any money or other compensation from, the payment processor administering the account, in exchange for referrals of business involving the debt relief services; and
- The consumer controls the funds in the account and can withdraw their funds from the debt relief service at any time without penalty and within seven (7) days from the consumer's request. [xxvii]

Example Scenarios – Violations of TSR

- *A payment processor's failure to pay to the consumer any interest earned on the consumer's funds held in a consumer's account at an insured financial institution;* [xxviii]
- *A payment processor's offer of, or a DSC's solicitation or receipt of, a financial consideration to the DSC such as a "technology implementation fee" or a free Customer Relationship Management (CRM) software, or any other consideration in partial or complete exchange for securing its payment processing business or referrals, i.e. in exchange for the DSC providing consumer enrollments to the payment processor.* [xxix]
- *A payment processor's offer of, or a DSC's solicitation or receipt of, financial incentives to the DSC in exchange for terminating contracts with existing payment processors, or for entering exclusive or near-exclusive contracts.* [xxx]



Business Affiliation

An important takeaway from the prohibitions of the TSR is the issue of the business relationship between the payment processor and the DSC. The TSR specifically bans any affiliation, ownership or control of the payment processor over the DSC for the purpose of ensuring an independent relationship between the DSC and the payment processor, to avoid conflicts of interest and to further protect consumers. [xxxi] Neither the FTC, the CFPB, nor the OCC provide any guidance on the definition of affiliation or control as stated in the TSR. However, the Federal Financial Institutions Examination Council (FFIEC), the interagency body of the FRB, FDIC, OCC and the CFPB, among others, is empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. The FFIEC defines "affiliate" as any company under common control with, or controlled by, that financial institution. The standard of "common control" is typically one or more persons who have 25%

voting or ownership of the company or controls the manner of the election of the board of directors. [xxxii] The Securities and Exchange Commission also defines an "affiliate" in Rule 405 under the Securities Act: "An affiliate of, or person affiliated with, a specified person, is a person that directly, or indirectly through one or more intermediaries, controls or is controlled by, or is under common control with, the person specified." The SEC finds that just a 10% interest (rather than 25%) can create affiliation.

In the context of financial arrangements, (a) a subsidiary is an entity that is more than 50% owned by another entity, and (b) control of an entity means the power, directly or indirectly, to vote a certain percentage (typically 5% or 10%) or more of the securities having ordinary voting power for the election of directors of the entity; or direct or cause the direction of the management and policies of the entity, whether by contract or otherwise. [xxxiii]

That the FTC chose not to define the exact parameters of an affiliated relationship or otherwise define "control" within the context of the DSC and payment processor relationship, suggests that the FTC views the prohibition broadly and the FTC has indicated that the TSR prohibitions on fee splitting or other compensation from a DSC to a payment processor should be applied broadly. See 75 Fed. Reg. 48458, 48490-91(2010). The FTC's use of the phrase "in any way affiliated with, the debt relief service" in 16 CFR §310.4(a)(5)(ii), further suggests that the relationship between the DSC and the payment processor be clearly an arms-length, independent relationship in which the processor does not have material ownership or control over the manner in which the DSC maintains consumer funds in a dedicated account.

Whether there are instances where a DSC and a payment processor can be "affiliated" in some manner and not violate the TSR remains an open question, although it is highly unlikely that such affiliation would not constitute a TSR violation. Much will depend not only on the relationship between the parties and how the parties interact with one another, but also upon how the relationship is structured, the extent to which the payment processor can influence decision-making by the DSC and the operations between the two parties. Until more guidance is provided by regulators, this is an area where both DSCs and payments processors will need to tread carefully.

Exemptions

The TSR provides some limited exemptions for companies that do not engage in telemarketing or that fall outside the specific criteria for "sellers" or "telemarketers." Some examples are as follows:

1. **Unsolicited Calls from Consumers** - Any call from a consumer that is not placed in response to a solicitation by the seller, charitable organization, or telemarketer;
2. **Calls Made in Response to a Catalog** - A call placed by consumers in response to a mailed catalog;
3. **Calls Made in Response to General Media Advertising** – A call made in response to general media advertising, such as TV commercials; infomercials; home shopping programs; radio ads; print ads in magazines, newspapers, the Yellow Pages, or online directories; and banner ads and other forms of mass media advertising and solicitation. *Telemarketers receiving these kinds of inbound calls from consumers are not exempt and have to comply with the TRS if the inbound call is in response to an advertisement for debt relief services*; and
4. **Calls Made in Response to Direct Mail Advertising** - Direct mail advertising includes, but is not limited to, postcards, flyers, door hangers, brochures, "certificates," letters, email, faxes, or similar methods of delivery sent to an identified person or family urging them to call a specified phone number about an offer of some sort, *but as noted the exemption does not apply to debt relief services*[xxxiv]

None of these exemptions would be applicable to any DSC as all communications

between a consumer and a DSC would involve debt settlement or debt relief services. Except with respect to prohibitions on misleading statements or activities, the TSR also does not apply to settlement of a business entity's (as opposed to a consumer's) debt.

Electronic Funds Transfer Act & Regulation E

Overview

Reg E implements the EFTA, which outlines the essential rights, liabilities, and obligations of consumers and institutions that offer electronic fund transfer and remittance services.[xxxv] The CFPB has the primary jurisdiction over Reg E.

General Applicability

The EFTA applies to any electronic fund transfer that authorizes a financial institution or other entity to debit or credit a consumer's deposit account, whether it be a savings or checking account. An "electronic fund transfer" (EFT) includes any transfer of funds initiated through an electronic terminal, telephone, computer, or magnetic tape to authorize a financial institution to debit or credit a consumer's account.[xxxvi] This includes transactions at ATMs, point-of-sale transactions, and preauthorized transfers such as direct deposits and automatic bill payments. Both a DSC and the payment processor can be deemed a financial institution under the EFTA and Reg E. When a DSC uses the services of a payment processor, the compliance responsibilities with the EFTA and Reg E fall upon both the DSC and payment processor at different touchpoints in the transfer process.

In 2021, the CFPB issued updated frequently asked questions (FAQs) regarding Reg E. [xxxvii] Two areas of focus were covered transactions and covered financial institutions. Reg E defines financial institutions to include not only traditional banks, savings associations, credit unions, but also any other person that ***directly or indirectly*** holds an account belonging to a consumer, or any other person that issues an access device and agrees with a consumer to provide EFT services. [xxxviii]. A DSC could be deemed a financial institution when it provides EFT services to consumers through a payment processor with a mechanism that facilitates the transfer of funds.

If a payment processor is holding a consumer's account, especially if they require a consumer working with a DSC to open a separate and designated account, then the payment processor is defined as a financial institution and subject to all the requirements of EFTA and Reg E, including providing required disclosures and establishing procedures for error resolution in the event of unauthorized transfers. In that instance, a DSC, as part of its oversight responsibilities, would need to ensure that the payment processor has the appropriate processes and procedures in place to ensure compliance with Reg E.

Required Disclosures

Pursuant to Regulation E, depending on who is holding the account or ultimately moving the consumer's money, disclosures must be provided at the time a consumer signs up for an EFT or before the first transfer involving the consumer's account.[xxxix] Typically the DSC would provide the initial disclosures to a consumer, since the DSC is working directly with the consumer. The payment processor should confirm delivery of the disclosures to the consumer by the DSC on behalf of the payment processor, especially if the payment processor is the one holding the account of the consumer and who's activities are such that the payment processor would be defined as a financial institution.

These disclosures must be clear, understandable, and provided in writing or in an electronic form that the consumer can retain. The initial disclosures must contain the following information:

1. **Consumer Liability**: A summary of the consumer's liability for unauthorized transfers, as defined by statute, relevant state or applicable laws or by agreement.
2. **Contact Information**: The telephone number and address for reporting potential unauthorized transfers.

3. **Business Days**: A statement of the financial institution's business days.
4. **Types of Transfers and Limitations**: A description of permitted electronic fund transfers and any limits on frequency or amount.
5. **Fees**: Any fees charged by the financial institution for electronic fund transfers or the right to make such transfers.
6. **Documentation**: A summary of the consumer's right to receipts, periodic statements and notices for preauthorized transfers
7. **Stop Payment**: A summary of the consumer's right to stop a preauthorized transfer and the stop-payment procedure.
8. **Institution Liability**: A summary of the institution's liability for failure to complete or stop specific transfers.
9. **Confidentiality**: The conditions under which the institution may share the consumer's account information with third parties.
10. **Error Resolution**: An error resolution notice, substantially similar to Model Form provide in the regulations.
11. **ATM Fees**: A notice that fees may be imposed by an ATM operator or by a network used to complete the transaction.

These disclosures must be updated if a new electronic fund transfer service, with different terms, is added to a consumer's account.[xl]

If a consumer agrees to preauthorized transfers at least once every 60 days, then the disclosures must be provided that inform the consumer of the multiple transfers, that require the written authorization by the consumer for the transfers, the schedule of the transfers, and the consumer's right to stop payment among other requirements. [xli] As noted above, typically the DSC would provide the disclosures for pre-authorized transfers but in the case where the payment processor is holding the account for the consumer, the DSC must ensure that the payment processor is provided with a copy of the written authorization of the preauthorized transfers. This prevents such transfers from being deemed unauthorized.

The CFPB has developed model disclosure forms for the disclosures.[xlii]

Error Resolution and Unauthorized Transfers

As a financial institution, either the DSC or the payment processor, as the case maybe, must comply with Reg E's requirements to have procedures in place to resolve errors that can occur and for any unauthorized transfer.[xliii] This includes providing to the consumer the ability to dispute the error or unauthorized transfer, to properly investigating the consumer's dispute of an error or unauthorized transfer, and to inform the consumer of the results of the investigation and any resolution therefrom. A DSC must ensure that the payment processor is adequately providing error resolution. In the 2021 FAQs, the CFPB, referencing a prior enforcement action against a bank, noted that an error investigation is not reasonable if the financial institution summarily denies error disputes if the consumer had similar error(s) with the same merchant.[xliv] DSCs and payment processors both have a duty to coordinate and investigate claims of errors by consumers. Neither party can delegate that responsibility to the other.

An unauthorized EFT is an EFT from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which

the consumer receives no benefit.[xlv] When payment processors debit fees through an EFT that are not properly disclosed or not otherwise permitted under applicable law, this can be deemed as an unauthorized transfer. (See, *Enforcement*). As will be discussed in the *Key Provisions in Contract Negotiations*, DSCs must be well aware of the charges and fees their payment processor partner will be assessing against their consumer clients. Improper charges or fees that should not be imposed, let alone transferred from a consumer's account, and the DSC's knowledge of same can result in significant liability. This is in addition to the DSC's responsibility for properly disclosing the terms of any settlement reached with a creditor and fees that will be charged to the consumer by the DSC for the DSC's services.

INDUSTRY RULES AND STANDARDS THAT DSCs AND PAYMENT PROCESSORS MUST CONSIDER

While payment processors are not generally subject to formal licensing apart from money transmission laws in many states, when processing credit or debit cards, all payment processors must comply with the Payment Card Industry Data Security Standard (PCI DSS)[xlvi] and adhere to specific industry rules established by individual payment card networks such as Visa, Mastercard, Discover, American Express and other card payment networks (Payment Card Network Rules).[xlvii]

Payment Card Industry Data Security Standards (PCI DSS)

Both DSCs and payment processors must be cognizant of important industry standards. While they do not have the force and effect of a law or regulation, noncompliance with these standards can result in significant operational disruptions or loss of the ability to process card payments, penalties and fines imposed by a payment card network, and reputational risk.

Payment processors are required to comply with the Payment Card Industry Data Security Standards (PCI DSS), a set of security protocols established to protect cardholder data (CHD). These standards apply to any organization that collects, processes, stores, or transmits debit or credit card information. Failure to comply with these standards can result in fines, penalties and potential loss of the ability to process card payments. [xlviii]

DSCs are responsible for ensuring their payment processor adheres to these requirements. Below are the key requirements of PCI DSS that payment processors must adhere to, and which DSCs must ensure are in place: [xlix]

1. **Firewall Configuration**: Payment processors must install and maintain a firewall configuration to protect cardholder data from unauthorized access.
2. **Unique System Passwords and Security Parameters**: Systems must use security parameters that are unique and not based on third-party defaults, ensuring stronger protection against unauthorized access.
3. **Protection of Stored Cardholder Data**: Any stored cardholder data must be securely protected to prevent breaches or misuse.
4. **Encryption of Cardholder Data Over Public Networks**: Cardholder data transmitted over public networks must be encrypted to safeguard it from potential interception or attack.
5. **Anti-Virus Software**: The processor must use and regularly update anti-virus software or programs to protect against malicious software that may compromise cardholder data.
6. **Secure System Development and Maintenance**: Payment processors must ensure the development and maintenance of secure systems and applications that mitigate vulnerabilities that could be exploited.

7. **Access Control Based on Need to Know**: Only authorized individuals should have access to cardholder data, and access should be limited to those with a legitimate need to know.
8. **Unique IDs for System Access**: Each individual with access to system resources should have a unique identification number to track and monitor actions within the system.
9. **Physical Access Restrictions**: Physical access to systems containing cardholder data should be restricted to authorized personnel only.
10. **Tracking and Monitoring Access**: There must be continuous monitoring and tracking of all access to network resources and cardholder data, ensuring accountability and timely detection of unauthorized access.
11. **Regular Security Testing**: Payment processors must regularly test their security systems and processes to identify and address vulnerabilities that may compromise data security.
12. **Information Security & Response Policy**: A comprehensive policy addressing information security must be maintained and communicated to all personnel involved in processing or handling cardholder data.

DSCs must ensure that their payment processors maintain these standards, as non-compliance could result in security breaches, financial penalties, or damage to the DSC's reputation. This will require regular assessments and monitoring of the payment processor's compliance with PCI-DSS.

NACHA Rules

Overview of NACHA Compliance

Payment processors must also comply with the rules established by the National Automated Clearing House Association (NACHA), which governs electronic payments made through the Automated Clearing House (ACH) network.[l] These rules, like the goals of Reg E, ensure secure, efficient, and transparent electronic fund transfers. When using the ACH network for payment processing, payment processors must adhere to NACHA's requirements, including authorization, risk management, and consumer protections, as well as operational rules that minimize fraud and errors. It must be remembered that NACHA is a not-for-profit association that develops the operating rules and business practices for any institution or business originating or receiving ACH payments. It is a compliment to the EFTA and Reg E and compliance with both the EFTA/Reg E and the NACHA rules are required.

General Applicability to DSCs

NACHA rules apply to any entity facilitating ACH transactions, including DSCs and payment processors, that debit or credit consumer accounts for payment settlement through the ACH Network. NACHA rules mandate obtaining proper authorization for debits, safeguarding sensitive consumer information, and promptly addressing unauthorized transactions. NACHA also emphasizes compliance with federal laws, such as Reg E, further tying its applicability to DSCs.[li]

Required Disclosures and Practices

Payment processors would do best to comply in all aspects with Reg E in order to be equally compliant with NACHA requirements. [lii] Additionally, NACHA outlines stringent measures for fraud prevention, transaction monitoring, and error resolution.[liii] DSCs should ensure that payment processors are integrating these requirements into their operations. The most effective way to ensure a payment processor is in compliance with these rules is to request to see the most recent NACHA audit[liv].

Payment Card Network Rules

Overview of Credit Card Core Rules

Visa Core Rules[lv], as well as the rules of Mastercard, American Express, Discover and other credit card networks (collectively the

"Rules") apply to the facilitation of all card-based transactions. These Rules cover a wide range of activities, such as transaction authorization, dispute resolution, and data security. For payment processors compliance is mandatory to maintain Visa or other card network access and to ensure that cardholder transactions are processed safely and efficiently. Noncompliance can result in penalties, fines, or even loss of access to the credit card network, presenting significant operational risks both for DSCs and payment processors.

Visa Core Rules are widely recognized as the industry standard and provide a clear framework for payment processors. The Rules of the other card networks are similar although they may vary in certain details. These Rules are all designed to ensure that payment processors, and other financial entities who process credit card payments, adhere to best practices for security, fraud prevention, and consumer protection.

For DSCs who accept credit cards through their payment processor, ensuring compliance with Visa's Core Rules and the Rules is essential, as these standards govern credit and debit card transactions critical to the debt settlement process.[lvi]

Pursuant to the Visa Core Rules, payment processors[lvii] must implement at a minimum the following practices:

1. **Transaction Authorization and Verification**[lviii]: Ensure all transactions are properly authorized and verified, mitigating fraud risks and protecting consumers.
2. **Chargeback and Dispute Management**[lix]: Establish robust processes for handling chargebacks and disputes, ensuring prompt resolution in compliance with Visa standards.
3. **Data Security**[lx]: Adhere to Visa's security requirements, including encryption and secure storage of cardholder data, to prevent breaches and unauthorized access.
4. **Risk Monitoring**[lxi]: Actively monitor transactions for fraud and unusual activity, leveraging tools provided by Visa to identify and mitigate potential risks.
5. **Transparency and Consumer Disclosures**[lxii]: Provide clear information about transaction terms, fees, and consumer rights, ensuring compliance with both Visa rules and applicable regulations like Reg E.

A DSC must ensure that the above practices are being integrated into a payment processor's operations to effectively manage its own third-party risk management obligations.[lxiii]

ENFORCEMENT

Overview

There have been significant enforcement actions both at the Federal and state levels against both DSCs and payment processors. Most have focused exclusively on direct violations of the TSR, EFTA and Reg E, the Consumer Financial Protection Act (CFPA) for unfair, deceptive, and abusive acts or practices, and various state consumer protection statutes. While the issue of oversight is usually not the sole basis of the enforcement action, the bad acts of one usually spawn scrutiny upon the other. This reinforces why third-party risk management is so important for DSCs. At a time when regulators have shown tremendous scrutiny upon the debt settlement industry, ensuring payment processing partners are not creating additional risk can only improve and support compliance efforts.

It is worth noting that despite the enhanced regulatory scrutiny, states and even federal regulators have provided little in the way of compliance guidance. This is not unusual, as regulators often tend to develop guidance through enforcement rather than through rulemaking or advisory opinions.

Federal Enforcement (CFPB & FTC)

There have been instances where the CFPB has taken direct action against payment processors for violations of law, including violations of the EFTA and Reg E.[lxiv] There have been no reported cases of the CFPB taking action against a debt settlement company for the actions of their payment processors, as their service providers. However, whether those same DSCs have been investigated or further supervised by the CFPB or other states is confidential in nature.

The FTC's enforcement actions with respect to the debt settlement industry and other types of debt relief services like student loan debt relief, as well as payment processors, is widely documented.[lxv] Most of these actions, like the CFPB, are brought independently upon each entity but the nature of the actions typically are the result of coordinated efforts of both the DSC and the payment processor.

It must be remembered that both the CFPB and the FTC have authority to enforce the Consumer Financial Protection Act (CFPA) [lxvi] and the FTC Act [lxvii], respectively, as well as rules and regulations promulgated pursuant to both, including the TSR. Both statutes prohibit unfair, deceptive and in the case of the CFPB, abusive acts and practices. Unlike the FTC, the CFPA can apply to service providers. There is nothing precluding the CFPB from bringing an action against a DSC for violations of the CFPA due to the conduct of its payment processors.

The CFPB has heavily scrutinized the activities of DCSs, as in the case of Strategic Financial Solutions [lxviii] and in conjunction with their relationships with payment processors. [lxix] The CFPB is increasingly taking a more aggressive enforcement posture with respect to both DSCs and their payment processors, with a view towards holding each as a gatekeeper against the other's non-compliance. Overall, the federal regulatory environment is nothing short of aggressive and will continue to be so, despite the change in administration. DSCs do not want to face enforcement scrutiny and consequences such as consent orders, judgments, fines and penalties, and even industry bars, due to their engagement with a non-compliant payment processor.

State Enforcement

Five years after the CFPB's enforcement action against Global Holdings, LLC (Global), the Massachusetts's Attorney General brought an action against both Global and Global's biggest customer, DMB Financial, LLC (DMB), for violations of the Massachusetts Consumer Protection Act.[lxx] This resulted in separate Consent Orders and an Assurance of Discontinue (AOD) against both DMB and Global, respectively.[lxxi] In the DMB matter, the Attorney General alleged that consumers were told to "make payments into a dedicated 'savings' account administered by Global." The AG touted the enforcement action against DMB as the "first-of-its-kind against a debt

settlement company in Massachusetts and its terms will lay out a roadmap for addressing misconduct in this industry going forward".[lxxii]

Shortly after the Massachusetts Consent Order, the CFPB then followed up with an enforcement action against DMB for violations of the TSR and CFPA

KEY PROVISIONS IN CONTRACT NEGOTIATIONS

When negotiating a contract with a third-party payment processor, DSCs must carefully consider specific terms to ensure that both operational and regulatory risks are effectively managed. A well-structured contract not only protects a DSC's interests but also sets clear expectations, establishes accountability, and outlines compliance standards that the payment processor must follow.

The OCC's Third-Party Risk Management handbook, based on the TPRM interagency guidance[lxxiii], is a useful resource in identifying key contractual elements to minimize potential risks for DSCs. The relevant provisions are outlined below.

Nature and Scope of the Arrangement

The contract should comprehensively outline the rights and responsibilities of both the DSC and the payment processor. Clearly defining these roles helps reduce ambiguity, minimize risk, and ensure seamless coordination. Important elements to cover include:

- Ancillary services, such as technology support, maintenance, and customer service;
- Specific activities of the payment processor will perform on behalf of the DSC;
- Terms governing access to and use of the company's information, facilities, systems, intellectual property, and equipment, along with any customer information.

Finally, as noted in the DMB enforcement action in Massachusetts, requiring consumers to only use one dedicated account administered by the payment processor was found to violate state law for unfair practices. This seems to suggest that exclusivity and lack of consumer choice may imply improper affiliation between a DSC and its payment processor which can be a violation of the TSR or other state law. If the scope of the relationship involves exclusivity or lack of the option by the consumer to choose an alternative payment processor, evidence of non-affiliation, control and ownership must be clearly articulated in the agreement.

Examples of some key terms follow:

Performance Measures or Benchmarks

Clear, measurable performance benchmarks should be established to gauge the payment processor's effectiveness and adherence to expectations and compliance with the law. These benchmarks enable the DSC to assess performance regularly and identify areas requiring attention.

Responsibilities for Information Access and Use

Both parties' roles in providing, receiving, and retaining information must be defined. The contract should include terms regarding information access, usage permissions, and restrictions on reselling, sharing, or reporting sensitive data.

Right to Audit and Require Remediation

The DSC should retain the right to conduct independent audits periodically to monitor compliance with and identify any issues that may require remediation. The contract should specify the types and frequency of these audits, ensuring they are sufficient for comprehensive oversight.

Compliance with Applicable Laws and Regulations

The contract must explicitly outline the payment processor's obligations to comply with relevant legal and regulatory requirements. Such specificity supports the DSC's regulatory compliance efforts and helps mitigate potential risks associated with non-compliance.

Cost, Compensation Structure and Fees

A clear compensation structure should detail schedules and calculations. Provisions for upfront and termination fees, along with responsibilities for additional costs, should also be included. Special attention must be made to ensure the DSC is not taking any upfront fees or that the payment processor is not debiting fees until it is appropriate to do so.

Ownership and Licensing

Ownership and licensing rights must be defined, particularly regarding any technology, information, or

intellectual property shared by the debt settlement company. This prevents potential conflicts over ownership or usage rights.

Confidentiality and Information Integrity

Given the sensitivity of non-public information, the contract must include strict confidentiality provisions to protect against unauthorized disclosure. It should also outline steps for reporting and addressing any breaches of information security.

Operational Resilience and Business Continuity

The contract should address operational resilience, outlining expectations for disaster planning, handling service interruptions, and cybersecurity. Provisions for continuity are essential to mitigate service disruptions that could impact customers or operations.

Indemnification and Limits on Liability

Responsibilities for claims and indemnification terms should be specified, defining each party's financial responsibilities and potential liabilities.

Insurance Requirements

The contract should stipulate the types and extent of insurance coverage required for the payment processor. Regular evidence of coverage may be necessary to ensure adequate protection.

Customer Complaint Handling

The responsibility of whether the DSC or payment processors, or some coordination of the two, will undertake the error resolution or investigation of an unauthorized transfer must be clearly articulated.

Regulatory Supervision and Oversight

The DSC's regulators may need access to the payment processor's operations to ensure compliance with applicable laws. The contract should confirm that the payment processor is subject to applicable regulatory examination and oversight.

Tailoring and Flexibility in Negotiation

While a standard contract may serve as a foundation, modifications or addendums are often required to address the unique complexities of the DSC's relationship with a payment processor. Adjusting the contract to meet specific risk profiles and compliance standards ensures that the DSC maintains adequate control and oversight throughout the contract lifecycle. Ensuring flexibility in the negotiation process allows for adjustments to maintain regulatory compliance, safeguard sensitive information, and protect the institution's interests.

CONCLUSION

The intricate regulatory landscape presents both challenges and critical responsibilities for DSCs and their payment processing partners. This whitepaper has underscored the importance of robust oversight, adherence to regulatory standards, and a proactive approach to managing these third-party relationships. While the debt settlement industry is uniquely positioned within the financial services sector, the principles of risk management and compliance drawn from regulatory requirements in the CFPB Act, the TSR and Reg E, along with the standards in the payments industry (PCI DDS, NACHA and Visa Network Rules) serve as the foundation for a secure and responsible business model.

In reviewing both the legal framework and practical challenges DSCs may face, including issues of transparency, contractual agreements, and regulatory compliance, this whitepaper highlights the essential practices that DSCs must adopt. Engaging payment processors does not reduce a DSC's responsibility to uphold consumer protections and compliance standards, even when functions are outsourced. By implementing the best practices and TPRM strategies outlined in this paper, DSCs can not only mitigate operational, financial and reputational risks but also contribute to a safer and more compliant debt settlement industry.

Clark Hill's Financial Services Regulatory & Compliance group is a national leader providing strategic legal counsel to clients in all areas of financial services law as well as representing those same clients during enforcement actions and examinations. Our clients include banks, financial institutions, fin-techs, private equity and venture capital firms, law firms, credit reporting agencies, and asset purchasers and sellers throughout the country.

Our support offerings to financial services clients include:

- Fractional Financial Services Regulatory Counsel
- Banking as a Service (BaaS) Advisory & Consulting
- Financial Services Innovation (FinTech), Product Consulting & Acquisition
- Compliance Management System (CMS) Risk Assessment and Due Diligence
- Regulatory Supervision & Investigation Readiness, Preparedness & Support
- Revenue Recovery Compliance Support

The financial services industry faces challenges on multiple fronts as it seeks to address compliance expectations from various financial services regulators. Our clients are subject to the jurisdiction of the Consumer Financial Protection Bureau (CFPB), the Federal Trade Commission (FTC), and prudential regulators like the Office of Comptroller of the Currency (OCC), the Federal Reserve Board (FRC), and the Federal Deposit Insurance Corporation (FDIC), as well state agencies and state attorneys general. In addition to our many offices around the country, our Washington, D.C. office allows our attorneys to stay on top of current developments, trends, and regulations affecting clients' business objectives and priorities.

We help clients navigate this rapidly evolving regulatory environment. Our exceptional team of lawyers and government and regulatory advisors have extensive experience and knowledge of the laws and regulations governing financial products and services. We can assist clients in developing and implementing compliance programs. Our lawyers work together in one multidisciplinary practice to bring a higher level of specialized knowledge and practical guidance.

OUR TEAM

Joann Needleman

Joann Needleman leads the firm's financial services regulatory and compliance practice and advises banks, financial institutions, and financial services entities on regulatory compliance matters.

(215) 640-8536

jneedleman@clarkhill.com

Aryeh Derman

Aryeh D. Derman supports and assists in the development and expansion of the regulatory and compliance group's growing consulting and advisory services, targeting financial institutions and technology companies (fin-techs) looking to enter into the financial services sector.

(312) 360-2508

aderman@clarkhill.com

Ryan Blumberg

Ryan Blumberg is a trusted advisor for banks, financial technology companies (FinTechs), and other financial institutions working within the dynamic realm of consumer financial services. Through his guidance, organizations can effectively navigate regulatory complexities, avoid potential pitfalls, and broaden their operational horizons. Widely respected nationally, Ryan is renowned for his profound experience in the FinTech domain and his adept representation of clients, earning recognition from both peers and satisfied customers alike.

(602) 440-4803

rblumberg@clarkhill.com

[i] https://www.consumerfinance.gov/ask-cfpb/what-is-a-debt-relief-program-and-how-do-i-know-if-i-should-use-one-en-1457/

[ii] *Operation Choke Point: Myths & Reality*, Administrative Law Review, 75.2, July 2023, https://administrativelawreview.org/wp-content/uploads/sites/2/2023/07/ALR-75.2_Stevenson.pdf

[iii] https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf

[iv] https://files.consumerfinance.gov/f/documents/102016_cfpb_OfficialGuidanceServiceProviderBulletin.pdf

[v] See, endnote (iii).

[vi] Id.

[vii] See, endnote (iv); 12 U.S.C. §§5515, 5514.

[viii] Id.

[ix] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

[x] https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know#Customer_information

[xi] https://www.occ.gov/news-issuances/news-releases/2024/pub-third-party-risk-management-guide-for-community-banks.pdf

[xii] *See*, OCC, Merchant Processing Handbook, https://www.occ.gov/topics/supervision-and-examination/credit/retail-credit/merchant-processing.html; FDIC Guidance on Payment Processer Relationship, (FIL-127-2008) https://www.fdic.gov/news/financial-institution-letters/2008/fil08127a.html#:~:text=Payment%20processors%20typically%20process%20payments,merchant%20clients%20to%20process%20transactions; NAICS Code 522320 (Financial Transactions Processing, Reserve, and Clearinghouse Activities); *see also*, https://tipalti.com/blog/payment-processor/.

[xiii] 31 U.S.C. §5330(d)(1)

[xiv] https://www.fincen.gov/money-services-business-msb-registration

[xv] Starting in January 1, 2026, Massachusetts will require a license for both foreign and domestic money transmissions; https://www.wolterskluwer.com/en/expert-insights/money-transmitter-business-license-requirements#form#gc

[xvi] Arizona Revised Statutes (ARS) § 6-1201 and Nevada Revised Statutes (NRS) § 671.013

[xvii] (https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/whether-company-provides-online-real-time

[xviii] 31 CFR 1010.100(ff)(5)(ii)

[xix] https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/definition-money-transmitter-merchant-payment

[xx] https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule

[xxi] 16 CFR Part 310

[xxii] 16 CFR 310.2(hh)

[xxiii] 16 CFR § 310.2(gg)

[xxiv] 16 CFR § 310 (ee)

[xxv] 16 CFR § 310.2(o)

[xxvi] 16 CFR § 310.3 & 16 CFR § 310.4

[xxvii] 16 CFR 310.4(a)(5)(ii)

[xxviii] 16 CFR 310.4(a)(5)(ii)(B)

[xxix] 16 CFR 310.4(a)(5)(ii)(D)

[xxx] 16 CFR 310.4(a)(5)(ii)(D)

[xxxi] 16 CFR 310.4(a)(5)(ii)(C)

[xxxii] https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/04

[xxxiii] https://content.next.westlaw.com/practical-law/document/I03f4d935eee311e28578f7ccc38dcbee/Affiliate?viewType=FullText&transitionType=Default&contextData=(sc.Default)

[xxxiv] 16 CFR 310.6(b)(5)

[xxxv] 12 CFR Part 1005

[xxxvi] 12 CFR Part 1005.3

[xxxvii] https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/

[xxxviii] 12 CFR 1005.2(i); a "person" means a natural person or an organization, including a corporation, government agency, estate, trust, partnership, proprietorship, cooperative, or association. See, 12 CFR 1005.2(j).

[xxxix] 12 CFR 1005.7

[xl] 12 CFR 1005.8(a)

[xli] 12 CFR 1005.10.

[xlii] Appendix A to Part 1005 — Model Disclosure Clauses and Forms; https://www.consumerfinance.gov/rules-policy/regulations/1005/a/

[xliii] 12 CFR 1005.11.

[xliv] https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/

[xlv] 12 CFR 1005.2(m).

[xlvi] https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

[xlvii] https://usa.visa.com/content/dam/VCOM/download/about-visa/visa-rules-public.pdf and https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/mastercard-rules.pdf

[xlviii] https://controller.ucsf.edu/how-to-guides/accounting-reporting/understanding-payment-card-industry-data-security-standard-pci

[xlix] https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

[l] https://nachaoperatingrulesonline.org

[li] https://www.nacha.org/content/how-ach-rules-are-made

[lii] NACHA Operating Guidelines Section I Chapter 2

[liii] https://nachaoperatingrulesonline.org/event-data/section/2024-nacha-operating-rules/2024-nacha-operating-rules_2

[liv] https://tipalti.com/resources/learn/nacha-rules/#what-is-a-nacha-audit

[lv] https://usa.visa.com/content/dam/VCOM/download/about-visa/visa-rules-public.pdf

[lvi] Visa Core Rules 1.5.2.

[lvii] Visa Core Rules 5.3.2.2

[lviii] Visa Core Rules 1.5.7.1

[lix] Visa Core Rules 1.5.4.14

[lx] Visa Core Rules 1.9.4.1

[lxi] Visa Card Acceptance Guidelines for Visa Merchants p. 54

[lxii] Visa Core Rules 1.5.1.3

[lxiii] https://www.occ.gov/news-issuances/news-releases/2024/pub-third-party-risk-management-guide-for-community-banks.pdf

[lxiv] https://files.consumerfinance.gov/f/201310_cfpb_meracord-proposed-stipulated-final-judgment-and-consent-order.pdf; https://files.consumerfinance.gov/f/201408_cfpb_consent-order_global-client-solutions.pdf; https://www.consumerfinance.gov/enforcement/actions/aci-worldwide-corp-and-aci-payments-inc/

[lxv] https://www.ftc.gov/system/files/documents/cases/first_data_filed_complaint.pdf; https://www.ftc.gov/system/files/documents/cases/interbill_final_order_as_to_tom_wells.pdf; https://www.ftc.gov/system/files/ftc_gov/pdf/x230038apexordermanzi.pdf; https://www.ftc.gov/system/files/documents/cases/complaint_7.pdf

[lxvi] 12 USC 5531; 12 USC 1036

[lxvii] 15 U.S.C. §§ 41-58

[lxviii] https://www.consumerfinance.gov/about-us/newsroom/cfpb-and-seven-state-attorneys-general-sue-debt-relief-enterprise-strategic-financial-solutions-for-illegally-swindling-more-than-100-million-from-financially-struggling-families/

[lxix] https://files.consumerfinance.gov/f/201504_cfpb_complaint-universal-debt.pdf; https://files.consumerfinance.gov/f/documents/cfpb_stipulated-final-judgment-order-universal-debt_2019-08.pdf

[lxx] https://www.mass.gov/doc/dmb-financial-final-judgement-0/download (Exhibit A)

[lxxi] https://www.mass.gov/doc/global-holdings-llc-aod/download; https://www.mass.gov/doc/dmb-financial-final-judgement-0/download

[lxxii] https://www.mass.gov/news/ag-healey-secures-1-million-in-first-of-its-kind-resolution-with-debt-settlement-company

[lxxiii] Third-Party Risk Management A Guide for Community Banks p.11 https://www.occ.gov/news-issuances/news-releases/2024/pub-third-party-risk-management-guide-for-community-banks.pdf