Federal and State Scrutiny of Payments

Payments Law Virtual Bootcamp – June 10, 2020

Ellen Berge, Partner, Venable
Andrew Bigart, Partner, Venable
Leonard Gordon, Partner, Venable

VENABLE LLP

Today's Discussion

- Overview of Federal Law Enforcement Scrutiny of Payments Industry
- Focus on Higher Risk-Areas
- Understanding Lessons Learned from Enforcement after Financial Crisis
- Recommended Practices for Minimizing Risk

VENABLE LLP

RFE4

Expect Continued Law Enforcement Scrutiny of the Payments Industry

VENABLE LLP

Law Enforcement in the Payments Industry

- Banks and processors are viewed as "gatekeepers" or "chokepoints" for fraudulent activity engaged in by merchants
- Continuing scrutiny of payments industry by Federal Trade Commission, Consumer Financial Protection Bureau, Department of Justice, and State Attorneys
  - FTC most active; does not have jurisdiction over banks, but cooperates with banking regulators
  - DOJ hired team of payments consultants to understand industry
- Note that federal regulators became increasingly active in targeting the payments industry following the 2008 financial crisis, particularly payments companies that were viewed as assisting merchants that were deceiving or taking advantage of vulnerable consumers

VENABLE LLP

State Law Enforcement

- Joint law enforcement with FTC
  - Recent law enforcement cases with Ohio attorney general, Florida attorney general
    - Unfair and deceptive practices stemming from merchant conduct
- State-regulated issues
  - Money transmission
- Other "consumer" protection
    - Equipment leasing
    - Payments processing agreements with small businesses

VENABLE LLP

Criminal Law Enforcement

- Department of Justice, U.S. Postal Inspection Service, Department of Treasury's Office of Foreign Assets Control (OFAC)
  - Conspiracy
  - False Statements to a Bank
  - Wire Fraud
  - Bank Fraud
  - Participating in Fraudulent Banking Activities
  - Conspiracy to Commit Money Laundering
  - Money Laundering
- Grand Jury Subpoenas
- PacNet Case (September 2016)
  - Designated as a significant transnational criminal organization (TCO) for processing for fraudulent/criminal direct mail scheme

OFAC

VENABLE LLP

"Chokepoint" Cases

VENABLE LLP

What Does Law Enforcement Look For?

- Credit card laundering
- Making false statements to a bank to obtain payment processing services
- Failing to disclose to processing partners material information about a merchant account, such as:
  - Identity of any owner, manager, director, or officer of the applicant for or holder of a merchant account
  - Any connection between an owner, manager, director, or officer of the applicant and a person who was previously terminated (due to chargebacks, fraud, questionable merchant status, merchant collusion, illegal transactions, or identity theft)
- Using a shell company and nominee owners to apply for a merchant account
- Using tactics to avoid fraud and risk monitoring programs
  - Load balancing sales transaction volume among multiple merchant accounts or merchant billing descriptors
  - Splitting a single sales transaction into multiple smaller transactions

VENABLE LLP

Types of Loss

Financial Loss	• Loss is the entire transaction • Chargebacks, fees, and assessments • In fraud situations, time and expense lost to investigate and remedy
Consumer Loss	• Loss is the total volume of sales processed • Plus potential fees paid to third parties (sales agents, banks) • Potential loss of reserves and suspended funds to the government • Consumer class action lawsuits • Criminal liability (illegal products)
Reputation & Operational Damage	• Loss of confidence / trust • Increased susceptibility to law enforcement or lawsuits • Court-ordered operating requirements

VENABLE LLP

Processor Liability ($)

- FTC seeks the full volume of sales transactions processed (less chargebacks and refunds)
- Example: $50 million sales processed = $50 million potential liability
- Cases often settle for less based on defendants making an "ability to pay" argument
  - Requires turnover of comprehensive financial statements completed on behalf of corporate and individual defendants
- FTC v. Universal Processing Services (11th Circuit) (December 2017)
  - Processors that collaborate with fraudulent merchants can be held jointly and severally liable for the full amount of sales processed by the merchant
  - The court rejected arguments that, in order to be held jointly and severally liable, a processor must be part of a "common enterprise" with the merchant

VENABLE LLP

Recent Enforcement Actions

- TransactPro (FTC, January 2020)
  - Foreign payment processor alleged to have helped defendants open multiple merchant processing accounts in the name of shell companies in order to evade credit card chargeback monitoring programs in connection with sale of "free trial" offers for personal care products and dietary supplements online
  - Imposition of $3.5 million judgment against processor and bans on providing payment processing services for certain categories of merchants
- RevenueWire (FTC, April 2020)
  - Defendant merchant was alleged to have engaged in card laundering by using its merchant processing account to process transactions for undisclosed businesses that were engaged in unlawful tech support scams

VENABLE LLP

FTC v. First Data Merchant Services

- FTC complaint and settlement filed May 2020
  - Defendants: First Data and former wholesale ISO, Vincent Ko (First Pay Solutions)
  - Related to unlawful merchant conduct in 2012-2014
- FTC allegations:
  - Unfair payment processing practices – opening accounts for shell companies, companies engaged in fraud, failed to timely terminate the accounts, ignored evidence of fraud
  - Credit card laundering – against Ko, under the Telemarketing Sales Rule
  - Allegation that First Data assisted the laundering
  - Assisting and facilitating deceptive representations in telemarketing

VENABLE LLP

Alleged Facts "Red Flags" in First Data Case

- First Pay Solutions (FPS), run by Vincent Ko, contracted with various sales agents or sub-ISOs in 2012-2014 to solicit high-risk merchants
  - Allegations that FPS failed to adequately underwrite or vet those sales agents
- Through sub-ISOs, FPS opened merchant accounts for businesses engaged in:
  - Deceptive telemarketing
  - Work-from-home schemes
  - Business coaching
  - Debt relief
  - One business enterprise that used stolen credit card data to bill consumers without consent

VENABLE LLP

Alleged Facts "Red Flags" in First Data Case

- Reference to hundreds of accounts under the names of shell companies
- Problems with application:
  - Facially false or deceptive information
  - Obvious factual discrepancies or inconsistencies
  - Omissions of key information
- FTC alleged identical applications submitted with the same information, used to load balance
- Websites that looked the same (same terms and conditions, same misspellings)
- Monitoring red flags:
  - Complaint alleges high refund and chargeback rates (27%-36%)
  - Continuing to process dispute warnings from law enforcement agencies and growing concerns from the sponsor bank

VENABLE LLP

First Data Settlement

- $40 million settlement
- New concepts in FTC settlement:
  - Detailed compliance requirements, but narrow applicability to "Covered Merchants" boarded by wholesale ISOs
    - Home-based internet business programs
    - Debt consolidation services
    - Sellers of nutraceutical products with a negative option feature

"Wholesale ISO" as defined by the FTC:

- Entered into an agreement with the processor and the bank
- Holds contractual liability to the bank and the processor for credit or fraud losses
- Has primary contractual responsibility for underwriting merchants and monitoring their transaction activity
- Does not include marketplaces or registered payment facilitators

VENABLE LLP

First Data Settlement

- Screening requirements for Covered Merchants
- Monitoring requirement for Covered Merchants
  - Submit reports on merchant investigations to third-party Assessor
- Wholesale ISO Oversight Program
  - Methodology for assessing risk levels of each wholesale ISO's merchant portfolio
  - Risk assessment for each wholesale ISO and prospective wholesale ISO
  - Risk ratings to current and prospective wholesale ISOs
  - Policies and procedures for overseeing the wholesale ISO's underwriting, monitoring, investigation, and adverse action as determined by the relevant risk rating
  - Routine reviews of chargebacks, intensive "shadow monitoring" and post-onboarding of a sampling of new restricted merchant applications, review
  - Monthly risk review of each wholesale ISO
  - Approval of all new restricted merchant marketing materials
  - Investigate and close accounts when necessary when wholesale ISO's portfolio generates chargebacks exceeding 0.75% / 75 count per month
  - Report to the third-party Assessor

VENABLE LLP

First Data Settlement

- Third-Party Assessor
  - Objective, independent third-party professional authorized to conduct Visa Global Acquirer Risk Standards (GARS) reviews or Mastercard Customer Risk Reviews
  - The FTC must approve First Data's selection of the Assessor
- Substantial responsibilities
  - Conduct an independent review of the Wholesale ISO Oversight Program, keep records relevant to the review for five (5) years after completion, and provide the documents to the FTC upon the FTC's request
  - Hire attorneys, investigators, accountants, and others to help with its duties
  - Have access to all information, documents, and personnel as necessary to carry out its duties
- Assessments to be done in phases

VENABLE LLP

FTC v. Qualpay

- June 2020
- Results from June 2018 FTC lawsuit against a business coaching and investment opportunity scheme
- Alleged failure to spot red flags in underwriting process
- Allegedly ignored monitoring red flags
- Continued to process up to FTC lawsuit
- FTC alleged unfairness

VENABLE LLP

Qualpay Settlement

- Monetary judgment of $46,779,358.91 (suspended due to inability to pay)
  - Qualpay must relinquish $6,314,342.09 in funds turned over to FTC receiver
- Ban on processing for certain merchant types: Business coaching and certain merchant types listed on MATCH list for excessive chargebacks, laundering, and other fraud reasons
- Screening and monitoring requirements for "high risk clients" defined to include:
  - Card-not-present merchants (processing more than $200K annually or more than 25% of sales as CNP)
  - Merchants selling a continuity program with a negative option feature
  - Multi-level marketing
  - Nutraceuticals
  - Scholarship finding services
  - Stored valued cards
  - Outbound telemarketing
  - Credit consolidation, debt restoration
  - Extended warranty programs
  - Government grants
  - Mortgage loan modification

VENABLE LLP

Other Hot Topics

VENABLE LLP

COVID-Related Products and Services

- Department of Justice
  - March 22, 2020, DOJ filed its first enforcement action against COVID-19 fraud, alleging that the operators of a website were unlawfully selling COVID-19 vaccine kits
  - April 29, 2020, DOJ obtained an injunction against websites fraudulently promoting and selling various silver products for the treatment and prevention of COVID-19
  - May 7, 2020, DOJ filed criminal complaint against website that offered telemedicine services for advertising and selling stolen COVID-19 testing services for $135 to $200, falsely claiming a connection to labs that would test the kits, shipping test kits without any prior medical screening, and providing no results to consumers
- Federal Trade Commission
  - Warning to over 100 marketers nationwide to stop making unsubstantiated claims that their products and therapies can treat or prevent COVID-19

VENABLE LLP

Financial Services for Vulnerable Consumers

- Following 2008 financial crisis, the DOJ, FTC, and other law enforcement organizations focused on targeting companies that were perceived to be taking advantage of vulnerable people
- With unemployment rising dramatically, and the potential for long-term financial repercussions from the pandemic, law enforcement may follow the same playbook in allocating its enforcement resources
- Potential targets for heightened scrutiny:
  - Consumer loans
  - Credit repair
  - Credit card protection
  - Identity theft protection
  - Debt collection, debt counseling, debt settlement, or debt consolidation
  - Mortgage or loan modification
  - Government grants
  - Foreclosure protection or guarantees
  - Multi-level marketing

VENABLE LLP

CBD

- The legality of CBD is complicated, with the product sitting at the intersection of numerous federal and state laws
  - According to the FDA, a dietary supplement, food, or drug containing CBD (derived from hemp or marijuana) violates federal law, unless the FDA has specifically approved an application or regulation authorizing the marketing of such product
  - In contrast, a ***cosmetic*** containing CBD may not violate the FDCA, as long as the CBD does not render the product injurious to users
- For merchants marketing hemp and CBD to consumers, there are also numerous federal (as well as state) laws that prohibit unfair or deceptive advertising and marketing practices, such as making false or unsubstantiated claims about the benefits of CBD
- The FDA and Federal Trade Commission (FTC) have warned purveyors of CBD oil that any claims that their product can prevent, treat, or cure human disease are required to be backed by reliable scientific evidence

VENABLE LLP

Small Businesses

- In 2019, the FTC announced a focus on deceptive acts and practices that harm small businesses
  - Examine trends and consumer protection issues in small business financing, including "proliferation of online loans and alternative financing products"
  - Expect focus on advertising and marketing
  - FTC has jurisdiction over advertising and marketing of small business loans under FTC Act in most instances, and some limited jurisdiction related to telemarketing of such loans, depending on the facts
- There has also been private litigation focusing on merchant processing practices (primarily fee disclosures, product add-ons, etc.) that are deceptive or unfair for small businesses

VENABLE LLP

Recurring Billing / Subscriptions

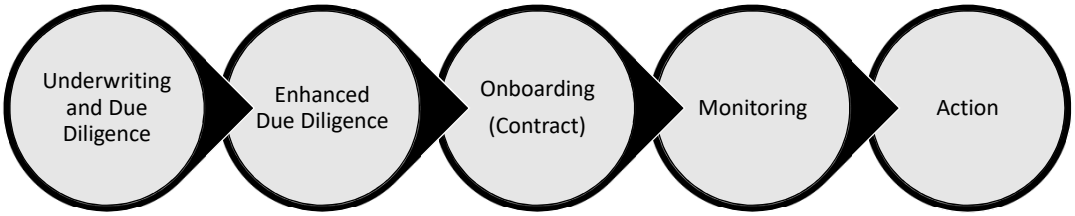
- During the pandemic, there is an increased reliance on recurring and subscription programs by consumers. This is an area that is subject to various federal and state laws
- Federal Law
  - Telemarketing Sales Rule (phone only)
  - Restore Online Shoppers Confidence Act (ROSCA) (internet only)
  - Section 5 of the FTC Act (all channels) (prohibits unfair and deceptive marketing practices)
- State Law
  - Automatic renewal laws in California, Virginia, Vermont, DC, other states
  - State notification laws (renewal notices)
  - "Mini FTC Acts"
  - Multi-state activity and class action risks

VENABLE LLP

Best Practices for Minimizing Risk

VENABLE LLP

Managing Merchant and Sub-merchant Risk



Policies and training should reflect the entire risk management life cycle.

VENABLE LLP

Compliance and Risk Management Basics

- Establish internal policies and procedures governing merchant acquiring program
  - Due diligence on prospective business partners
  - Requirements, limitations, and prohibitions for merchant acquiring activities
  - Shadow monitoring of business partner and merchant activities
  - Auditing of business partners
  - Management reporting
  - Training
- Draft contracts with business partners that flow down card brand requirements, compliance requirements, reporting requirements, and audit rights, among other standard provisions
- Regular review of merchant acquiring program to identify areas of weakness and opportunities for improvement

VENABLE LLP

Underwriting and Due Diligence Red Flags

- Use of shell companies and nominee owners
  - Opening straw accounts using "nominee" owners who have no actual involvement in the merchant business
  - Opening multiple accounts through multiple banks and ISO channels to load balance volume and chargebacks
    - Attempt to identify related accounts
- Incomplete merchant applications
- Evidence of consumer complaints, past law enforcement actions, prior bank or card network warnings, high-risk credit report
- Deficient merchant sales and cancellation policies, marketing practices, customer services, and other factors

VENABLE LLP

Monitoring of Merchant Accounts

- Traditionally, processing statistics and chargeback activity was the primary way to identify merchant fraud or unsatisfactory account performance
- Today, there are heightened regulatory expectations of monitoring practices. This means shadow monitoring of business partner and merchant activities (PFs, merchants, etc.)
- The objectives of merchant risk management:
  - Identify and investigate merchant activity that is abnormal for your expectations for the merchant
  - Identify and investigate activity that is atypical for industry norms for general merchant processing and for defined verticals
  - Ensure merchant compliance with Card Brand requirements
  - Support the identification of suspicious activities that may be related to money laundering or terrorist financing
  - Identify anomalous activity and file a Suspicious Activity Report with the Financial Crimes Enforcement Network (FinCEN) or bank, when appropriate

VENABLE LLP

Monitoring of Merchant Accounts

- Best Practices
  - Scrutinize requests to open multiple accounts
  - Obtain beneficial ownership information
  - Monitor accounts for relatedness (names, addresses, products, etc.)
- Monitor for Red Flags
  - High chargebacks and returns (by count and ratio)
  - Use of dummy websites
  - Opening multiple MIDs to load balance chargebacks
  - Splitting transactions: (1) sales, (2) shipping, (3) processing
  - Submitting merchant applications with nominal owners
  - Frequent movement between high-risk banks/processors/ISOs
  - "Cascading" through multiple merchant accounts to resubmit declined transactions

VENABLE LLP

Monitoring of Merchant Accounts

- Do not board merchants in violation of policies and procedures
- Terminate Merchants / PFs / etc. when appropriate
  - If processing activity reaches a level of greater concern and investigation reveals that the merchant is engaging in practices that could be considered unfair, deceptive, or abusive to consumers, that merchant should be terminated
  - Watch for partners engaged in repeat onboarding of "bad" merchants

VENABLE LLP

Andrew Bigart
(202) 344-4323
AEBigart@Venable.com

Ellen Berge
(202) 344-4704
ETBerge@Venable.com

Leonard Gordon
(212) 370-6252
LLGordon@Venable.com

VENABLE LLP