Cutting Out the Middleman: Holding Third-Party Payment Processors Liable for the Acts of Their Merchant Clients

BROOKE KETTLER*

TABLE OF CONTENTS

INTRODUCTION .......................................... 1723

I. SHORT-TERM PREDATORY LENDING AND THE ROLE OF THE THIRD-PARTY PAYMENT PROCESSOR ........................................ 1724
A. SHORT-TERM PREDATORY LENDING ..................... 1724
1. The Line Between Short-Term Lending and Predatory Short-Term Lending ........................... 1724
2. The Problem of Short-Term Predatory Lending 1725
3. Types of Short-Term Predatory Lending and Their Harms ..................................... 1727
4. Combating Short-Term Lending Schemes & Lender Evasion ........................................ 1729
B. THE ROLE OF THE THIRD-PARTY PAYMENT PROCESSOR IN SHORT-TERM LENDING SCHEMES ....................... 1731
1. Focus on the Third-Party Payment Processor ........ 1731
2. How Payment Processing Works ....................... 1732
   a. The Third-Party Payment Processor’s Role in Lending ........................................ 1733
   b. Payment Processing Systems ........................ 1733

II. THEORIES OF LIABILITY FOR THIRD-PARTY PAYMENT PROCESSORS ........................ 1736
A. AIDING AND ABETTING .............................. 1736
1. Standards for Aiding and Abetting ................. 1737
   a. Actual Knowledge ............................ 1737

* Georgetown University Law Center, J.D., 2017; Washington University in St. Louis, B.A., Political Science and Psychology, 2014. © 2017, Brooke Kettler. Special thanks to Professors Mansfield and Peller for sharing their expertise, and to the editors and staff of The Georgetown Law Journal for their helpful comments and suggestions during the development of this Note.
b. Substantial Assistance ................................. 1737

2. Case Law: Aiding and Abetting by Third-Party Payment Processors .......................... 1738

3. Finding Liability for Third-Party Payment Processors of Predatory and Abusive Lenders .......................... 1738
   a. Actual Knowledge ............................... 1739
      i. The Merchant Application ................. 1739
      ii. Monitoring Systems ...................... 1742
      iii. Red Flags ............................... 1743

   b. Substantial Assistance .......................... 1744

B. NEGLIGENT INFLICTION OF ECONOMIC LOSS ............................. 1746

1. Doctrine ........................................ 1747
   a. General Rule Against Recovery ............. 1747
   b. Exceptions ................................. 1747

2. Application to Third-Party Payment Processors ........ 1749
   a. Elements .................................. 1749
   b. Duty ..................................... 1750
      i. Merchant Application ...................... 1750
      ii. Monitoring Systems ...................... 1752
      iii. Red Flags ............................... 1753
      iv. Institutional Recommendations .......... 1754
   c. Breach of Duty ............................. 1755

3. Argument for Extending Exceptions .................... 1756

III. VERMONT LAW AS A MODEL FOR OTHER STATES .......................... 1757

CONCLUSION ........................................ 1759

“I’m never going to get off this merry-go-round. I wish I’d never gotten these loans.” — Lisa Engelkins, Payday Lending Victim

INTRODUCTION

The first payday loan that Sandy took out “was for $100, with an $18 fee.”\(^2\) Soon, she found herself with multiple loans, taking out new loans to pay off the fees due on her prior loans.\(^3\) Sandy became trapped in an all-too-common cycle of debt, paying $300 every two weeks on four different payday loans.\(^4\) She continued to borrow for months until she eventually “lost her job and could no longer keep up with the fees” owed on her loans.\(^5\) Eventually, Sandy was forced to file for bankruptcy.\(^6\)

Sandy’s story is not unique. Every year, thousands of consumers fall victim to abusive, predatory, or unlawful short-term lending schemes. Although some victims have been able to recoup losses through litigation, many consumers find themselves unable to recover due to the difficulty of suing these lenders directly. To obtain redress, consumers need an alternative way to hold those responsible for their losses accountable. This Note argues that one potential recourse for wronged consumers is to hold the middlemen in these short-term lending transactions—third-party payment processors (payment processors)—liable for the abusive and predatory acts of their merchant clients. Payment processors, the intermediaries that initiate debits from consumers’ bank accounts on behalf of lenders, play an essential role in short-term lending and should be liable for the harm to consumers. Holding payment processors liable will provide a form of recovery to the victims of predatory and abusive short-term loans who otherwise might be hundreds—or thousands—of dollars out of pocket with no hope of recuperation.

This Note is divided into three distinct Parts with respective subsections. Section I.A discusses the short-term lending system. Specifically, it explains the short-term lending system, the harm that predatory and abusive short-term lending causes, and the difficulty of holding short-term lenders liable themselves. Section I.B addresses the role of the third-party payment processor in the short-term lending system and the possibility of focusing liability on payment processors as a means to gain redress for consumers unable to recover directly against lenders. Part II details potential theories of liability for third-party payment processors working on behalf of lenders. Section II.A explores aiding and abetting liability. It outlines the standards for proving aiding and abetting liability, discusses case law addressing aiding and abetting liability for payment processors, and explains how aiding and abetting liability could be applied to payment processors in the context of predatory and abusive lending. Section II.B discusses negligent infliction of economic loss. It details the doctrine of negligent infliction of economic loss, explores how it could be applied to

\(^2\) Id.  
\(^3\) Id.  
\(^4\) Id.  
\(^5\) Id.  
\(^6\) Id.
payment processors, and discusses why the doctrine—which is usually not entertained by courts—should be permitted as a cause of action against payment processors in the context of predatory and abusive lending. Part III suggests that other states should follow Vermont’s lead in holding payment processors directly liable by statute for processing payments in violation of state consumer protection laws.

I. SHORT-TERM PREDATORY LENDING AND THE ROLE OF THE THIRD-PARTY PAYMENT PROCESSOR

A. SHORT-TERM PREDATORY LENDING

This section focuses on (1) the benefits of non-abusive short-term lending and how it can become abusive, (2) the problem of short-term predatory lending, (3) types of short-term predatory lending and the associated harm, and (4) regulatory and litigious attempts to combat predatory short-term lending schemes and the methods abusive lenders use to evade those attempts. It concludes that although short-term lending may be necessary for individuals who need access to cash in an emergency, predatory and abusive short-term lending causes consumers substantial harm that existing mechanisms have failed to prevent or redress.

1. The Line Between Short-Term Lending and Predatory Short-Term Lending

Although short-term loans are regularly offered in a predatory or abusive manner, short-term lending is not inherently abusive or unlawful.\(^7\) This Note does not propose eradicating all forms of short-term lending. Instead, it suggests focusing liability on third-party payment processors as a means of stopping predatory and abusive short-term lending practices. The goal of focusing on payment processors is to protect consumers by limiting abusive practices and simultaneously allowing legitimate lenders to continue offering loans so that individuals with limited borrowing choices have the option to take out a short-term loan in emergencies.

Not all short-term loans are offered in a predatory or abusive way,\(^8\) and many defend them as an essential resource for individuals with few other ways to seek credit.\(^9\) Supporters of the short-term loan industry argue that such loans offer a

---

\(^7\) See, e.g., Protections from Predatory Short-Term Loans, CORP. FOR ENTER. DEV. 1 (Oct. 2012), http://cfed.org/assets/scorecard/2013/rg_PredatoryLending_2013.pdf [https://perma.cc/7U5U-NYST] (“Although installment loans are not an inherently predatory product, they become predatory when finance companies charge excessive fees and interest rates and continually pressure customers to refinance and take out new loans.”).

\(^8\) See id. But see Payday Loans are Often a Last Resort for the Poor. That Doesn’t Mean They Should be Exploitive, LOS ANGELES TIMES (June 3, 2016), http://www.latimes.com/opinion/editorials/la-ed-payday-loans-20160602-snap-story.html [https://perma.cc/4AYY-P8MZ] (explaining that fourteen states have banned payday lending because they find it “inherently abusive”).

solution for cash-strapped individuals who need to cover an unexpected expense. Short-term loans can help people cover the costs of an unexpected financial burden, such as a medical emergency or a home repair. Those individuals may have no other choice but to take out a payday loan rather than, for example, face eviction for a missed rent payment. In some cases, a short-term loan, such as a payday loan, may be less expensive than an alternative, such as an overdraft fee from a bank. Faced with other expensive options for obtaining credit, cash-strapped individuals may see a short-term loan as preferable.

While short-term lending may offer a necessary service for consumers in need of quick cash, problems with short-term lending arise when it becomes abusive and predatory. Although some short-term lenders look out for consumer interests, others flagrantly ignore the best interests of the consumer. So, although some short-term lenders operate legitimate businesses that aim to provide a necessary service in a professional and lawful manner, at least some lenders aim to “profit through avoidance of industry norms or legally prescribed limits.”

2. The Problem of Short-Term Predatory Lending

When short-term lending becomes predatory, it causes substantial harm to consumers. Every year, about 12 million Americans take out small dollar, short-term loans, spending a collective average of $7.4 billion. This harm largely stems from predatory short-term lending’s imposition of “unfair and abusive loan terms on borrowers,” particularly in the form of unfair fees and
exceptionally high interest rates.\textsuperscript{18} Predatory lenders typically target moderate and low-income consumers, often leaving these consumers and their families with fewer resources.\textsuperscript{19} Because most predatory loans are marketed without full disclosure of costs and terms, consumers are at a high risk of unintentionally contracting for the harsh consequences of a predatory loan.\textsuperscript{20} In addition, the lenders’ incentives generally undermine the needs of the borrower.\textsuperscript{21} Short-term, high-interest loans are “‘designed to trap individuals in long-term debt’ and have a ‘devastating impact on families’ financial well-being.’”\textsuperscript{22}

The harm predatory short-term lending causes consumers is multifold. In addition to the substantial amount the consumer often initially pays, predatory lending can cause injury such as overdraft and bounced check fees, the burden of closing bank accounts, opening new bank accounts, ordering new checks,\textsuperscript{23} and the process of challenging and reversing debits.\textsuperscript{24} Overdraft fees can cause further loss to consumers by triggering additional overdrafts and associated fees.\textsuperscript{25}

Predatory lenders set high fees and interest rates without consideration of the borrowers’ ability to repay.\textsuperscript{26} This system makes it difficult for consumers to fully pay off a previous loan while covering their regular expenses.\textsuperscript{27} Borrowers become trapped in a cycle of debt where they cannot repay their loan and must take out additional loans to pay off previous ones.\textsuperscript{28} For example, 75\% of payday loans are taken out to cover an original loan the borrower was unable to repay.\textsuperscript{29} Many borrowers remain in debt for up to a year on their so-called

\textsuperscript{18.} Id. at 26 (listing common characteristics of predatory lenders).
\textsuperscript{20.} See \textsuperscript{id} at 8 (listing misaligned incentives as a sign of abusive lending).
\textsuperscript{21.} \textsuperscript{JUSTIN KOLBER & WENDY MORGAN, VT ATTORNEY GEN.’S OFFICE, ILLEGAL LENDING, FACTS AND FIGURES 3} (2014) (quoting \textit{CTR. FOR RESPONSIBLE LENDING, EFFECTIVE STATE AND FEDERAL PAYDAY LENDING ENFORCEMENT: PAVING THE WAY FOR BROADER, STRONGER PROTECTIONS 1} (Oct. 4, 2013)).
\textsuperscript{23.} See \textit{Complaint, FTC v. Landmark Clearing, Inc., supra note 23, at ¶ 17} (noting that unauthorized debiting may force a consumer to have to undertake the process of reversing debits).
\textsuperscript{25.} \textsuperscript{See \textit{PROTECTIONS FROM PREDATORY SHORT-TERM LOANS, supra note 7}, at 1.}
\textsuperscript{26.} \textsuperscript{See \textsuperscript{PAYDAY LENDING IN AMERICA, supra note 16}, at 1.}
\textsuperscript{27.} \textsuperscript{See \textsuperscript{Balassone & Wroblewski, supra note 16}, at 1.}
\textsuperscript{28.} \textsuperscript{See \textsuperscript{Kolber & Morgan, supra note 22}, at 3.}
In addition to imposing unfair and abusive terms and interest rates on consumers, short-term lending may involve illegal activity. For example, loans may violate state usury caps. In New York, loans violate civil usury laws where they impose an APR higher than 16% and, in Vermont, no person may charge an interest rate greater than 12–24% APR (depending on the type of loan). Lenders might also evade state licensing laws. For example, all lenders must obtain a state license from the Vermont Department of Financial Regulation to make loans. Internet lenders, however, often attempt to circumvent state usury and licensing laws by offering loans over the Internet to consumers residing in states where their loans would be unlawful. A lender may even be operating a fraudulent business. A lender may engage in fraud by unlawfully obtaining consumer account information and using that information to debit consumer accounts without the consumer’s authorization or full understanding.

3. Types of Short-Term Predatory Lending and Their Harms

Short-term predatory lending comes in many forms, including payday lending, car title lending, tax refund anticipation loans (RALs), and abusive installment loans.

Payday lending is one of the most pervasive forms of predatory lending, with approximately 12 million Americans borrowing nearly $50 billion through the

---

30. See id.
31. See Jean A. Fox & Anna Petrini, Consumer Fed’n of Am., Internet Payday Lending: How High Priced Lenders Use the Internet to Mine Borrowers in Debt and E evade State Consumer Protections 7–8 (Nov. 30, 2004), http://www.consumerfed.org/pdfs/Internet_Payday_Lending113004.PDF [https://perma.cc/83C8-ER8X] (explaining that many states ban payday lending under state usury laws, while many others limit the annual interest that lenders may charge).
32. See N.Y. Gen. Oblig. § 5-501 (McKinney 2011) (referencing the interest rate limit established in N.Y. Banking § 14-a (McKinney 2012), which is 16%). In addition, a loan in New York violates criminal usury laws where the interest rate is greater than 25%. N.Y. Penal § 190.40 (McKinney 2016); see also Complaint at ¶ 8, Hillick v. BMO Harris Bank, No. 13-CV-1222 (N.D.N.Y. dismissed Dec. 16, 2013).
33. See 9 V.S.A. § 41a (2016).
34. See 8 V.S.A. § 2201 (2012).
35. See The Pew Charitable Trusts, Fraud and Abuse Online: Harmful Practices in Internet Payday Lending 22 (2014), http://www.pewtrusts.org/~/media/assets/2014/10/payday-lending-report/fraud_and_abuse_online_harmful_practices_in_internet_payday_lending.pdf [https://perma.cc/8VBZ-CE2L]. For example, online lenders may “incorporate in a state with permissive lending laws and... attempt to circumvent rate caps in more restrictive states by effectively exporting the interest rate rules of their home states.” Id.; see also Complaint, Hillick v. BMO Harris Bank, supra note 32, at ¶¶ 2–3 (describing how online payday lenders circumvent state usury laws).
payday loan industry each year. Payday loans are short-term, high interest loans. To obtain a payday loan, the borrower provides the lender with a post-dated check or authorizes electronic debit access to their account. These loans come with exorbitantly high interest rates—up to 574% in some states. The average borrower is charged about $15 per $100 borrowed per two weeks, and pays about $520 in interest each year. The cycle of debt is particularly harsh in the realm of payday lending, with only about 2% of payday loans going to borrowers who are able to pay off their loan by the first due date. With so many consumers trapped in this cycle of debt, about 76% of payday loans are attributable to borrowers who are “unable to repay one loan without taking a new loan during a two-week period.” As of 2016, payday lending was either banned, or effectively prohibited, in fourteen states and the District of Columbia. With the movement to online lending, however, many payday lenders have been able to circumvent applicable state laws.

Another form of predatory short-term lending is car title lending. Car title loans are small, short-term loans, usually no more than a few hundred dollars. The average fees and interest rates for a car title loan are equivalent to about 400% APR. A consumer obtains a car title loan by signing over the title of their vehicle. If the borrower defaults on the loan, the lender may take possession of and sell the vehicle. These loans put what might be a family’s most valuable asset—their car—at risk. That risk is frighteningly high because car title loans have exceptionally high interest rates and, like payday loans, may

40. See Peterson, supra note 38. Interest rates on payday loans can range from about 196% in Minnesota to 574% in Mississippi. Id.
41. See PAYDAY LENDING IN AMERICA, supra note 16, at 6.
42. See id. at 4; see also Protections from Predatory Short-Term Loans, supra note 7, at 1.
43. See Protections from Predatory Short-Term Loans, supra note 7, at 1.
44. LESLIE PARRISH & URIAH KIND, PHANTOM DEMAND: SHORT-TERM DUE DATE GENERATES NEED FOR REPEAT PAYDAY LOANS, ACCOUNTING FOR 76% OF TOTAL VOLUME, CTR. FOR RESPONSIBLE LENDING 6 (Jul. 9 2009) http://www.responsiblelending.org/payday-lending/research-analysis/phantom-demand-final.pdf [https://perma.cc/KFC8-4PAZ].
46. See, e.g., Hunter Stuart, Payday Lenders Are Using the Internet to Evade State Law, HUFFINGTON POST (Jan. 12, 2015), http://www.huffingtonpost.com/2015/01/12/payday-lenders_n_6443134.html [http://perma.cc/6AWQ-VCNB] (“Many of these companies claim that because they operate online, state law doesn’t apply to them.”).
47. See Protections from Predatory Short-Term Loans, supra note 7, at 1.
48. See id.
49. See id.
50. See id.
51. See id.
52. See id.
cause consumers to fall into a cycle of debt.\textsuperscript{53} Unable to pay off the loan the first time it is due, the average borrower renews the loan approximately eight times, incurring significant interest costs.\textsuperscript{54}

Consumers may also fall victim to tax refund anticipation loans (RALs) and abusive installment loans. RALs are short-term cash advance loans that are taken against a consumer’s expected income tax refund.\textsuperscript{55} RALs impose high interest rates, ranging from about 40\% to over 700\% APR.\textsuperscript{56} Installment loans are loans that are paid back in monthly installments, plus interest.\textsuperscript{57} They are offered on a variety of debts, including cars, homes, and college degrees.\textsuperscript{58} Installment loans may become predatory when finance companies charge excessive fees and interest rates, and encourage consumers to refinance or take out additional loans.\textsuperscript{59}

4. Combatting Short-Term Lending Schemes & Lender Evasion

There have been two primary approaches in regulation and litigation to combatting short-term lending schemes: targeting the lenders themselves and targeting the lenders’ service providers, which include banks and third-party payment processors.\textsuperscript{60} Unfortunately, “focusing solely on the lenders is often inefficient and ineffective,” because “[m]any of these lenders operate online, have several affiliated companies, and change their business names often, all to obscure both their location and the true lender-in-interest.”\textsuperscript{61}

Other lenders have been able to reach borrowers via the Internet in states that prohibit, or effectively prohibit, various types of lending.\textsuperscript{62} In 2012, the revenue generated by online short-term lending increased by 14\%, comprising 40\% of short-term lending.\textsuperscript{63} The recent popularity of online lending has complicated

\begin{flushleft}
\textsuperscript{53.} See Protections from Predatory Short-Term Loans, supra note 7, at 1.
\textsuperscript{54.} See Aff. of John Robinson at ¶ 43, In re TitleMax Holdings, 447 B.R. 896 (Bankr. S.D. Ga. 2009) (No. 09-40805) (specifying that the average thirty-day loan—the product at the core of Title-Max’s title-loan business—is renewed eight times); see also Protections from Predatory Short-Term Loans, supra note 7, at 1.
\textsuperscript{55.} See Refund Anticipation Loans, supra note 37.
\textsuperscript{56.} See id.
\textsuperscript{58.} See id.
\textsuperscript{59.} See Protections from Predatory Short-Term Loans, supra note 7, at 1.
\textsuperscript{60.} See Balassone & Wroblewski, supra note 16, at 10. Various regulatory agencies can take direct action against short-term lenders. For example, under The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), the Consumer Finance Protection Bureau (CFPB) has regulatory, enforcement, and supervisory authority, and the FTC wields enforcement power over consumer financial protection and UDAP laws; also, many states attorneys general have the authority to bring action against online short-term lenders. \textit{Id.}
\textsuperscript{62.} See Kolber & Morgan, supra note 22, at 5.
the enforcement of short-term lending laws. Specifically, it raises questions about if and when online lenders must be licensed in the state where the borrower resides, and if and when the state usury laws of the borrower’s state apply to the loan.64 Lenders are often able to reach borrowers in states that prohibit, or effectively prohibit, certain forms of short-term lending by offering loans over the Internet.65 Many states argue that out-of-state lenders are obligated to comply with the laws of their state when dealing with residents of their state and have attempted to apply usury and licensing laws to online lenders operating within their state.66 Various federal agencies, such as the Federal Trade Commission (FTC), federal banking agencies, and the Department of Justice (DOJ), as well as many private class action lawyers have made similar arguments.67 Although many states have attempted to apply the law of the borrower’s home state to online transactions, their attempts have often been thwarted.68

Another common way that lenders evade state laws is by acting through banks.69 By working with federally insured depository institutions that have exportation and preemption privileges, lenders are able to evade state usury laws, payday loan laws, and small loan rate caps.70 The lenders enter into arrangements with banks by which the lender issues the loan, the bank quickly sells back most of the loan obligation, and the lender advances the money and collects the debt.71 Through these “rent-a-bank” arrangements, lenders are able to issue loans that do not comply with state consumer protection laws.72 For example, California law prohibits checks used in loans to exceed $300; but, by partnering with banks, lenders are able to make loans that exceed that limit.73

In addition, some lenders (often online lenders) are owned and operated by Native American tribes, which, because of their status as sovereign entities, are immune from suit in federal or state court.74 Loan agreements with tribal
lenders generally select tribal law as the governing law, making regulation and bringing suit even more difficult. Other lenders “are located off-shore and in foreign countries, adding further complications for enforcement.” Lenders located in other countries may argue their loans are subject to the laws of the country in which they are physically located.

B. THE ROLE OF THE THIRD-PARTY PAYMENT PROCESSOR IN SHORT-TERM LENDING SCHEMES

This section first explains why the regulatory focus concerning abusive short-term lending has shifted to third-party entities such as payment processors, rather than solely on the lenders themselves. It also provides an explanation of how third-party payment processing works in the specific context of lending. This section aims to provide a picture of the complicated world of payment processing and to show the significant role that a third-party payment processor occupies in short-term lending.

1. Focus on the Third-Party Payment Processor

As a result of the difficulty of bringing direct action against the lenders themselves, focus has shifted to the entities that enable lenders to operate, such as banks and third-party payment processors. Particularly in the aftermath of the economic downturn, there has been more scrutiny on third-party payment processors as various agencies try to protect financially insecure consumers.

Third-party payment processors are not per se illegal, nor is there anything per se illegal about most of the merchants they contract with. However, in addition to unlawful acts taken directly by some third-party payment processors, payment processors may “deliver services to clients that engage in deceptive, abusive, or illegal practices.” Third-party payment processors play a crucial role in lending transactions, giving lenders access to consumer ac-

75. See Balassone & Wroblewski, supra note 16, at 2; Kolber & Morgan, supra note 22, at 5.
76. Letter from Justin E. Kolber to Marsha Jones, supra note 61, at 3.
77. See Fox & Petreni, supra note 31, at 22.
78. See Balassone & Wroblewski, supra note 16, at 2 (“In light of these challenges to bringing direct actions against the lenders themselves, the focus has shifted to cutting off those lenders’ access to entities that provide services to them, such as banks, debt collectors, marketing providers, and credit bureaus.”).
79. See FTC Press Release, supra note 23.
counts.83 For example, an out-of-state payday lender would not be able to circumvent state usury laws that prohibit payday lending without the assistance of third-party payment processors.84

The U.S. financial and economic system relies on the payment system.85 People rely on the banking and third-party payment processing system to protect them from unlawful schemes.86 Accordingly, many see stopping the payment processors’ “facilitation, along with preventing other payment system violations,” as “vital to protecting consumers across the country,” particularly “where state laws outlaw abusive lending practices.”87

2. How Payment Processing Works

Payment processing plays a central and highly integrated role in the exchange of money between borrowers and lenders. A third-party payment processor is a non-bank payment processor that manages payments on behalf of merchants.88 In the typical third-party payment processor relationship, the payment processor is a deposit customer of a bank.89 The payment processor uses its account to initiate debit transactions from consumer accounts on behalf of its merchant clients. After the payment processor receives the funds from a consumer’s account, it sends the money to the merchant’s account.90 The third-party payment processor’s clients usually do not have a direct relationship with the payment processor’s bank.91 The third-party payment processor serves as the intermediary between the payee (the lender), who is the payment processor’s customer, and the bank that requests payment from the check clearing or automatic clearing house system (ACH).92

83. See Press Release, U.S. Attorney’s Office E.D.N.C., United States Attorney Announces Settlement with Bank Accused of Consumer Fraud (Apr. 29, 2014) (noting “[p]ayment processors provide to a wide variety of merchants access to the national payment system,” taking money out of consumers’ accounts and depositing the money into its merchant client’s account) https://www.justice.gov/usao-ednc/pr/united-states-attorney-announces-settlement-bank-accused-consumer-fraud [https://perma.cc/7X78-KYMR]; see also Complaint, Hillick v. BMO Harris Bank, supra note 32, at ¶ 6 (explaining the role of banks in facilitating payday lending in states where such loans are unlawful or enforceable).
84. See id. (explaining the essential role that banks play in helping payday lenders circumventing state usury laws).
85. See Press Release, Senator Jeff Merkley, Bicameral Group of Members Urge DOJ to Crack Down on Consumer Scams (Feb. 26, 2014) (“The nation’s payment system . . . is the backbone of the U.S. financial and economic infrastructure.”).
86. See id.
87. Id. Congressmen wrote a letter to Attorney General Holder urging him to scrutinize “potential payment fraud, anti-money laundering violations, and other illegal conduct involving payments by banks and third-party payment processors” to prevent illegal lending. Id.
88. See FinCEN, FIN-2012-A010, supra note 81.
89. See FDIC FINANCIAL INSTITUTION LETTER, supra note 36, at 1.
90. See LAUREN K. SAUNDERS ET AL., CONSUMER BANKING AND PAYMENTS LAW § 3.13.3 (2013).
91. See FinCEN, FIN-2012-A010, supra note 81.
92. See SAUNDERS ET AL., supra note 90, § 3.13.3; see also ANA R. CANAZOS-WRIGHT, AN EXAMINATION OF REMOTELY CREATED CHECKS 4 (2012).
Traditionally, third-party payment processors have contracted with domestic storefront retailers to process transactions such as credit card payments, ACH transactions, remotely created checks (RCCs), and debit and prepaid card transactions.93 The Internet has enabled third-party payment processors to expand their client base and now work on behalf of both domestic and international merchants, operating via storefront as well as online.94

a. The Third-Party Payment Processor’s Role in Lending. The third-party payment processor has a central role in the lending process. When a borrower contracts with a lender, the loan is deposited into the consumer’s account. If the loan is issued online, lenders “either transmit demands for withdrawal through their own financial institution or use a third-party processor, which handles loans for multiple lenders, and its financial institution, referred to as the ‘originating bank.’”95 The originating bank then debits the consumer’s account for prepayment owed on the loan.96 In these transactions, “[t]he processors know their clients are lenders of high-interest internet loans or payday loans.”97

b. Payment Processing Systems. Most third-party payment processors process payments through the ACH system or through the creation of RCCs,98 both of which are more susceptible to fraud than other payment forms, such as traditional checks.99

The ACH system is a “batch-processing, store-and-forward system” in which banks collect ACH requests throughout the day and subsequently transmit them to a central clearinghouse in batches.100 The banks then transfer the appropriate amounts into the transferees’ bank accounts.101 An ACH transfer can be initiated orally, in print, or electronically.102 The transfers themselves are sent electronically between banks and other institutions.103

An ACH “entry” is an “electronic item representing the transfer of funds in the ACH.”104 It is a request by one party in the ACH to another for a credit or 

---

93. See FinCEN, FIN-2012-A010, supra note 81.
94. See id.
95. Kolber & Morgan, supra note 22, at 6.
96. Id.
97. Id.
98. See Conference of State Bank Supervisors, supra note 82, at 2; see also FDIC Financial Institution Letter, supra note 36, at 1.
99. Cf. FDIC Financial Institution Letter, supra note 36 (explaining that financial institutions should exercise greater care and implement more stringent safeguards when handling RCC and ACH transactions to prevent fraudulent or criminal transfers).
100. See Saunders et al., supra note 90, § 5.1.5.2.
102. See Saunders et al., supra note 90, § 5.1.5.2.
103. See id.
debit transfer. The party initiating the entry (the Originator) can only initiate the entry upon authorization from the consumer. After obtaining authorization, the Originator authorizes the bank to send the ACH entry to the consumer’s account. The bank receiving orders from the originator forwards the entry to the ACH operator, which sends the entry to the consumer’s bank, which posts it to the consumer’s account.

Some merchants and lenders use a third-party payment processor to gather information from consumers and initiate entries on behalf of the merchant or lender. A third-party payment processor initiates an ACH debit transfer on behalf of a merchant client by submitting the transfers to the payment processor’s bank. The merchant provides the third-party payment processor with information about the consumer that the payment processor needs to initiate the debit transfer, such as the consumer’s routing and account numbers. Upon receipt of the transfer order, the bank enters the order into the ACH network.

Remotely created checks “do not bear the signature of a person on whose account the payments are drawn.” A remotely created check differs from a traditional check in that the payee, rather than the account holder, creates the instrument that directs the paying bank to make a payment. To authorize an RCC, an account holder provides his or her routing and account numbers to the merchant, who subsequently passes the information to the third-party payment processor.

Rather than create a check itself, the payee may use a third-party payment processor to create and deposit a remotely created check into an account held by

---

105. An entry can be a “credit” transfer, in which funds are “pushed” from the consumer’s account, or a “debit” transfer, where funds are “pulled” from the consumer’s account pursuant to instructions from the business. See Saunders et al., supra note 90, § 5.1.5.2.

106. See id. Where a consumer has set up an electronic bill payment, the consumer is the originator, because they are the party that initiated the ACH entry and requested that funds be pushed from his or her account and transferred to the receiving company. Id.; see also NACHA Operating Guidelines, supra note 101, § V, ch. 38, at OG59.

107. See Saunders et al., supra note 90, § 5.1.5.2; NACHA Operating Rules—Corporate Edition § 2.3.1, OR5 (2013) [hereinafter NACHA Operating Rules].

108. See id.

109. See id.; NACHA Operating Guidelines, supra note 101, § I, ch. 1, at OG5. The ACH Operator transmits and received ACH entries. See Saunders et al., supra note 90, § 5.1.5.3; NACHA Operating Rules, supra note 107, § 2.3.4, at OR7. It is usually the Federal Reserve Bank in the Originating Depository Financial Institution’s (ODFI’s) district. See Saunders et al., supra note 90, § 5.1.5.3.

110. See Saunders et al., supra note 90, § 5.1.5.2.


112. See id.

113. Id. See also RCC Payment Processing Risky for Banks, NationalACH.com (Mar. 7, 2012), http://www.nationalach.com/rcc-payment-processing-risky-for-banks/ [https://perma.cc/3GWT-5V3P] (the lack of a signature on an RCC makes the payment method more vulnerable to fraud).

114. See Cazazos-Wright, supra note 92, at 1–2.

115. See Saunders et al., supra note 90, § 3.13.3.
the payee or by the payment processor acting as an agent of the payee. The lender sends the third-party payment processor the information needed to create a paper check, which the payment processor then creates and deposits into its own bank account. In some cases, the third-party payment processor acts on behalf of another third-party payment processor, attenuating the connection between the original payee and the bank that originates the payment. In the payment processing world, RCCs are commonly associated with high-risk merchants and pose a higher risk of processing fraudulent payments. Rather than bear a customer’s authorizing signature, a RCC includes a phrase such as “authorized by the drawer.”

In addition, the third-party payment processor may use the new technology of a remotely created payment order transaction (RCPO). An RCPO is processed through the banking system in a manner similar to a paper check. Unlike a paper check, however, an RCPO is an electronic image created by the payment processor, not the merchant and, unlike an RCC, “never existed in paper form.” Like an RCC, however, an RCPO does not have a consumer’s signature and instead includes a statement such as “authorized by the drawer.”

To create the RCPO, the third-party payment processor needs express authorization from the consumer. But the payment processor need not prove to the consumer’s bank that it has such authorization; it only needs to claim that it has such authorization on file. In an RCPO with a third-party payment processor, the consumer provides her name, bank account information, and authorization to the merchant, who then passes that information to the payment processor. The third-party payment processor then creates the RCPO and transmits it to the payment processor’s bank for deposit. The bank sends the RCPO image through the check clearing system to the consumer’s bank, which then debits the consumer’s account and sends the funds to the payment processor’s account. After deducting a fee and setting aside funds to serve as a reserve against

---

117. See Saunders et al., supra note 90, § 3.13.3.
118. See id.
120. See FinCEN, FIN-2012-A010, supra note 81.
122. See id.; see also Complaint, FTC v. Landmark Clearing, Inc., supra note 23, at 7 (explaining further the function and similarities of RCCs and RCPOs).
123. See FinCEN, FIN-2012-A010, supra note 81, at 4 (explaining that an RCPO is “an RCC that never existed in paper form and is processed through the check system from the outset as an electronic check image,” and that an RCC “was not created by the consumer or her bank”).
124. Id. at 6.
125. See id. (explaining that RCPOs and RCCs look the same).
returns, the third-party payment processor sends the rest of the money to the merchant client.\textsuperscript{126}

II. THEORIES OF LIABILITY FOR THIRD-PARTY PAYMENT PROCESSORS

Lender evasion has made it more and more difficult to hold lenders themselves directly liable. As a result, millions of consumers are left without redress for the multitude of harms that they suffer from the often unlawful and abusive practices of short-term predatory lenders. As an alternative way to find justice, consumer victims might sue the lenders’ third-party payment processors for the role the payment processors play in enabling the lenders to engage in predatory schemes. Section II.A will address the possibility of holding third-party payment processors accountable under a theory of aiding and abetting. Section II.B will consider a cause of action for negligent infliction of economic loss.

Section II.A concludes that consumers can establish aiding and abetting liability for a third-party payment processor by showing the payment processor had actual knowledge of its lender client’s predatory, abusive, and unlawful activity and that the payment processor substantially assisted its lenders client’s wrongdoing. Section II.B concludes that consumers can establish liability under the doctrine of negligent infliction of economic loss by showing that the payment processor had actual knowledge of its lender client’s predatory, abusive, and unlawful activity and that the payment processor breached its duty of care by continuing to process payments despite knowing about its lender client’s wrongdoing.

A. AIDING AND ABETTING

This section proposes that one possible way to hold a third-party payment processor liable for harm incurred by borrowers is to show that the payment processor aided and abetted the unlawful or abusive acts of its lender client. Under a theory of aiding and abetting, plaintiffs would assert that the third-party payment processor aided and abetted the violation of state consumer protection laws. Specifically, this section will (1) explain the elements of an aiding and abetting claim; (2) discuss case law holding third-party payment processors liable for aiding and abetting in areas other than lending; and (3) consider the possibility of finding third-party payment processors liable specifically for aiding and abetting lenders. This section concludes that consumers can establish actual knowledge for aiding and abetting liability by showing that the payment processor was on notice of its lender client’s wrongdoing via the merchant application, monitoring system, red flags, or both. It further finds that consumers can establish the substantial assistance prong of aiding and abetting liability by showing that the payment processor engaged in “ordinary business transac-

\textsuperscript{126} See id.
tions” on behalf of the lender, gave the lender credibility, or enabled the lender to access funds.

1. Standards for Aiding and Abetting

Under the doctrine of aiding and abetting, a third party can be held liable for harm done by another party where the third party “[1] knows that the other’s conduct constitutes a breach of duty and [2] gives substantial assistance or encouragement to the other so to conduct himself.”127 These elements are often referred to as “actual knowledge” and “substantial assistance.”128 Where aiding and abetting liability is established, the aider and abettor “is himself a tortfeasor and is responsible for the consequences of the other’s act.”129

a. Actual Knowledge. To sufficiently plead a theory of aiding and abetting liability, the plaintiff must allege actual knowledge such that the defendant was “generally aware of his role as part of an overall illegal or tortious activity.”130 Actual knowledge requires a subjective awareness that the wrongdoer’s conduct constitutes a breach of duty owed to others.131 Actual knowledge does not require specific intent—the plaintiff need not show proof of an agreement to commit the primary wrong.132 Aiding and abetting “is only intentional in the sense that the aider and abettor intends to take the actions that aid and abet, not that the tortfeasor specifically intends for his actions to result in the fraudulent harm.”133

b. Substantial Assistance. In addition to establishing actual knowledge, the plaintiff must establish that “the defendant... knowingly and substantially assist[ed] the principal violation.”134 Even ordinary business transactions undertaken with actual knowledge that the transaction is part of a wrongful operation

127. Restatement (Second) of Torts § 876(b) (Am. Law Inst. 1979); see also Brief of Amicus Curiae Attorney General of Wash. at *12, Carlsen v. Global Client Solutions, No. 84855-6, 2011 WL 720803 (Wash. Feb. 22, 2011).

128. See Casey v. U.S. Bank Nat’l Ass’n, 26 Cal. Rptr. 3d 401, 405–06 (Cal. Ct. App. 2005) (describing the elements of aiding and abetting as substantial assistance to a wrongdoer with actual knowledge that the other’s conduct constitutes a breach of duty).

129. Restatement (Second) of Torts § 876(b) cmt. d.; see also Newton v. Am. Debt Servs., No. 11-3228, 2013 WL 5592620, at *4 (N.D. Cal. Oct. 10, 2014) (explaining that under a theory of aiding and abetting, the aider and abettor is liable as a co-tortfeasor for the wrong); Brief of Amicus Curiae Attorney General of Wash., Carlsen v. Global Client Solutions, supra note 127, at *12.

130. Halberstam v. Welch, 705 F.2d 472, 477 (D.C. Cir. 1983). Civil aiding and abetting differs from other forms of joint and several liability in that it focuses on “whether a defendant knowingly gave ‘substantial assistance’ to someone who performed wrongful conduct.” Id. at 478.


133. In re First Alliance Mortg. Co., 471 F. 3d 977, 1005 (9th Cir. 2006).

are sufficient to find there was substantial assistance.\footnote{In re First Alliance Mortg. Co., 471 F.3d at 994–95 (quoting Casey v. U.S. Bank Nat’l Ass’n, 26 Cal. Rptr. 3d 401, 406 (Cal. Ct. App. 2005)); \textit{see also} Plaintiff’s Memorandum in Opposition to Gateway’s Motion to Dismiss, Ray v. BlueHippo Funding, \textit{supra} note 131, at *6 (quoting \textit{In re First Alliance Mortg. Co.}, 471 F.3d at 994–95).}

2. Case Law: Aiding and Abetting by Third-Party Payment Processors

Case law has established that a third-party payment processor may be found liable under a theory of aiding and abetting its merchant client’s conduct. In \textit{Carlsen v. Global Client Solutions}, the Supreme Court of Washington found that a third-party payment processor was liable as an aider and abettor of an unlawful debt adjustment settlement program in violation of Washington’s debt adjustment statute.\footnote{256 P.3d 321, 324 (Wash. 2011); \textit{see also} WASH. REV. CODE ANN. § 18.28.190 (2016).} In an amicus brief, the Washington Attorney General argued that a payment processor should face civil aiding and abetting liability for aiding and abetting unlawful debt settlement companies where the debt settlement companies violated state law, the payment processor knew that the debt settlement companies were violating state law, and the payment processor substantially assisted in the violation of state law.\footnote{See Brief of Amicus Curiae Attorney General of Wash., Carlsen v. Global Client Solutions, \textit{supra} note 127, at #13.} The Washington Attorney General’s logic in his \textit{Carlsen} brief can be applied to find a third-party payment processor liable for the commission of a wrong by the payment processor’s lender client. Like debt settlement companies’ unlawful actions were evidence of the payment processor’s liability in \textit{Carlsen}, commission of a wrong by a lender is evidence of a breach of duty by its payment processor. Where the third-party payment processor is generally aware that the lender is violating a statute, and where the payment processor substantially assists the lender, the payment processor should be found liable for civil aiding and abetting.\footnote{\textit{See id.} (arguing that a payment processor should be held liable for aiding and abetting unlawful debt settlement companies if the debt settlement companies were violating state law, the payment processors knew that the companies were violating state law, and the payment processors substantially assisted in the violation of state law).}

3. Finding Liability for Third-Party Payment Processors of Predatory and Abusive Lenders

To establish aider and abettor liability against a third-party payment processor working on behalf of its merchant client, the merchant client must have committed a wrongful act, the payment processor must know of the wrongful act, and the payment processor must have substantially assisted the merchant in that wrongful act.\footnote{See \textit{Restatement (Second) of Torts} § 876(b) (AM. LAW INST. 1979); Brief of Amicus Curiae Attorney General of Wash., Carlsen v. Global Client Solutions, \textit{supra} note 127, at *12 (explaining that to find the payment processors liable for an unlawful debt settlement scheme under a theory of aiding and abetting, there must be proof of a wrongful act by the debt settlement companies, knowledge by the


\footnote{136. 256 P.3d 321, 324 (Wash. 2011); \textit{see also} WASH. REV. CODE ANN. § 18.28.190 (2016).}

\footnote{137. \textit{See Brief of Amicus Curiae Attorney General of Wash., Carlsen v. Global Client Solutions, \textit{supra} note 127, at #13.}}
a. Actual Knowledge. In establishing a claim for aiding and abetting liability against a third-party payment processor, plaintiffs may argue that the payment processor had actual knowledge of the wrongful acts by its lender clients by way of the payment processor’s review of the merchant application, its monitoring systems, and various other red flags. A strong argument can be made that when a third-party payment processor works with an abusive or unlawful lender, the payment processors know that its lender clients are engaged in abusive or unlawful activity.\textsuperscript{140}

i. The Merchant Application. Before agreeing to process payments on behalf of a lender, the third-party payment processor receives a merchant application from the lender. Information in that application may alert the payment processor, from the start, to the abusive or unlawful activity of its potential client. Various government offices have suggested that payment processors have, or should have, detailed information about the merchants that they contract with in their merchant applications. In a letter from the Office of the Comptroller of the Currency (OCC) to banks, the OCC suggested that banks “require the processor to provide information on [its] merchant clients, such as the merchant’s name, principal business activity, and geographic location.”\textsuperscript{141} In addition, they suggest that banks verify with the payment processor that the merchant’s business is lawful.\textsuperscript{142} In its own guidance to banks, the Federal Deposit Insurance Corporation (FDIC) suggested that banks request information about the merchant clients from the third-party payment processors, including “the merchant’s name, principal business activity, location, and sales techniques.”\textsuperscript{143} The OCC’s and FDIC’s suggestions indicate that the payment processor has such information on hand. If, however, the current practice in the payment processing industry does not include the collection of this information, an increase in banks requesting the information from third-party payment processors in light of the OCC and FDIC guidance may spur payment processors to incorporate the collection of the requested material as part of its ordinary protocol; in turn, payment processors that the debt settlement companies were breaching a duty, and the payment processors must have substantially assisted the debt settlement companies in the wrongful act); see also Halberstam v. Welch, 705 F.2d 472, 478 (D.C. Cir. 1983) (explaining the plaintiff must show three elements: “(1) the party whom the defendant aids must perform a wrongful act that causes an injury; (2) the defendant must be generally aware of his role as part of an overall illegal or tortious activity at the time he provides the assistance; (3) the defendant must knowingly and substantially assist the principal violation”).

140. \textit{See KOLBER & MORGAN, supra note 22, at 6 (explaining that when third-party payment processors transmit payments for a lender, they “know their clients are lenders of high-interest internet loans or payday loans”).}


142. \textit{See id.}

143. FDIC Financial Institution Letter, \textit{supra} note 36, at 5.
adoption of that practice would result in a higher likelihood of knowledge. The information that should be contained in the merchant application, such as prior actions against the merchant, the merchant’s field of business, ISO referrals, and other suspicious information, help establish that the payment processor had actual knowledge of the merchant’s wrongdoing.

The merchant’s application should include basic information about the lender, such as the lender’s name. With that information, the payment processor can undertake basic due diligence to determine if the lender has been involved in any prior civil, criminal, or regulatory investigations or actions.144 Where the lender’s practices have been the subject of consumer protection investigations and lawsuits, the prior investigations and lawsuits give the payment processor “actual knowledge” of the merchant’s wrongdoing.145 In *Reyes v. Zion First Nat’l Bank*, plaintiffs sufficiently pled that a payment processor knew that its clients were engaged in fraudulent telemarketing because the telemarketers in question were known to have engaged in similar fraud in the past.146 Similarly, a third-party payment processor may know that its clients are engaged in abusive or unlawful activity because of involvement in analogous activity in the past.

The application should also enable the third-party payment processor to deduce the lender’s field of business. Certain categories of merchants are generally considered to be of higher risk than others, which should put payment processors on notice to look out for suspicious activity. For example, online merchants tend to have a higher risk profile because those clients “tend[] to display a higher incidence of consumer fraud or potentially illegal activities than some other businesses.”147 In addition, the characteristics of out-of-state payday lenders put a third-party payment processor on notice of the lender’s unlawful activity. ACH debits originated from out-of-state payday lenders raise red flags that notify the payment processor of the unlawful activity.148 In *Hillick v. BMO Harris Bank*, the complaint alleged that, where a defendant bank that

144. See generally Michael Bernardo et al., Chief, Cyber Fraud and Financial Crimes Section, FDIC, Third Party Payment Processors: Relationships, Guidance, and Case Examples, Presentation to the Federal Financial Institutions Examination Council (Sept. 17, 2013) (suggesting due diligence banks should undertake with regard to both merchants and third-party payment processors).
146. See id.
147. FDIC FINANCIAL INSTITUTION LETTER, supra note 36, at 1; see also FinCEN, FIN-2012-A010, supra note 81.
initiated entries on the ACH network knew the out-of-state payday lender’s identity, that the lender was a payday lender, and that the lender was making payday loans in a state that prohibits such loans, the defendant bank “knew” that the lender was engaged in unlawful activity. The *Hillick* plaintiffs’ analysis with regard to lenders contracting with banks can be extended to lenders contracting with third-party payment processors.

The merchant application may tell the third-party payment processor that a client was referred from an Independent Sales Organization (ISO). ISOs and third-party payment processors sometimes enter relationships in which the ISOs solicit and refer clients to the payment processor. Where an ISO has referred predatory clients in the past, the payment processor has reason to be more suspicious of future clients referred by the same ISO.

The face of the merchant application may also contain other clear indicia of unlawful or abusive behavior. In *Universal Debt & Payment Solutions*, the Consumer Financial Protection Bureau (CFPB) sued third-party payment processors, alleging aiding and abetting of its merchant clients’ fraud. The CFPB alleged that, although the application listed the merchant’s home address as his business address and conveyed a credit history that was unacceptable under the payment processor’s standards, the payment processor approved the application. The payment processor also approved an application for a merchant that listed a physical and legal address it never occupied, included an address on a voided check with the application that belonged to another collection agency, and faxed “the application . . . from a FedEx Office location.”

Even where a third-party payment processor receives a merchant’s application with no immediate indicia of wrongful activity, the lender may still be running a suspicious business. The payment processor can easily verify whether the merchant is running a legitimate business by comparing the information on the application with public record databases and fraud databases or by comparing it to information held by a third party (such as a consumer reporting agency). Where the payment processor discovers that the merchant is engaged in unlawful activity, the payment processor has obtained actual knowledge sufficient to plead the first element of aiding and abetting liability.

---

149. See Complaint, *Hillick v. BMO Harris Bank*, *supra* note 32, at ¶¶ 94, 164. The analysis holding banks liable for their role in unlawful and abusive lending can be applied to hold payment processors liable for their role in unlawful and abusive lending. Third-party payment processors act as a middleman between the banks and the lender, adopting a role similar to that of the bank.


152. See id. at *30–31.


154. See *OCC BULLETIN* 2008–2012, *supra* note 141 (suggesting that banks verify the legitimacy of a merchant’s business through these techniques).
ii. Monitoring Systems. In addition to indications of suspicious activity that arise via the merchant application at the outset of a payment processing relationship, third-party payment processors may become aware of abusive or unlawful behavior during the course of their relationship with a lender. Payment processors may have in place voluntary or contractual monitoring systems that should alert them to unlawful or suspicious activity by lender clients.\textsuperscript{155} The monitoring system may include “policies, procedures, and processes to determine the adequacy of due diligence standards for new merchants.”\textsuperscript{156} Specifically, the third-party payment processor might check the lender’s references and verify a physical address for the operation of the business.\textsuperscript{157}

In its complaint against Universal Debt Solutions, the CFPB alleged that third-party payment processors of phantom debt collectors “knew” that the debt collectors were unlawful, in part because the payment processors “ignored their own stated policies concerning whether to approve the debt collectors’ applications.”\textsuperscript{158} Instead of, or in addition to, a self-imposed monitoring system, a third-party payment processor may contract with its bank to monitor for suspicious activity such as high return rates.\textsuperscript{159} In an action against a third-party payment processor alleging unfair acts or practices, the FTC noted the payment processor’s contract with its bank that required the payment processor to investigate the past return rates of prospective merchant clients before contracting with them.\textsuperscript{160} Further, the FDIC suggests that banks enter into written contracts with third-party payment processors that specify each party’s responsibilities.\textsuperscript{161} The FDIC’s recommendation likely means that there are a substantial number of these contracts.

Additionally, various agencies have suggested that payment processors should have risk assessing measures in place. For example, the FDIC has stated that “payment processors must have effective processes for verifying their merchant

\begin{footnotes}
156. FDIC FINANCIAL INSTITUTION LETTER, supra note 36, at 4.
159. See Complaint, CFPB v. Universal Debt & Payment Solutions, LLC, supra note 151, at ¶ 3. In suing payment processor involved in phantom debt collection scheme, CFPB alleged that the payment processor had contracted with its bank to monitor chargebacks, and that it had failed to investigate suspicious activity on the debt collectors’ accounts). See id. at ¶ 34.
161. See FDIC FINANCIAL INSTITUTION LETTER, supra note 36, at 1.
\end{footnotes}
clients’ identities and reviewing their business practices.”

Similarly, the Vermont Attorney General’s Office has written letters to various entities asking them to urge third-party payment processors to undertake due diligence procedures. In a letter to the Third Party Payment Processors Association (TPPPA), the Assistant Attorney General of Vermont requested help in combating illegal and predatory lending and informed the TPPPA about Vermont’s laws affecting third-party payment processors. He also sent a letter to the National Automated Clearing House Association (NACHA) seeking assistance in combatting illegal and predatory lending, asking that “NACHA advise all payment processors to prevent unauthorized consumer loan transactions.”

iii. Red Flags. In the course of a payment processing relationship, “red flags” such as complaints and high return rates may arise that may bolster the third-party payment processor’s knowledge that the lender is engaged in abusive or unlawful practices such as customer complaints and abnormally high return rates.

One strong indicator of questionable merchant activity is a high volume of customer complaints alleging that the client is wrongfully obtaining personal account information, misleading customers, misstating prices, or charging undisclosed or unauthorized fees. Consumers often submit complaints directly to the payment processor, helping to ensure that the payment processor is aware of the alleged wrongdoing. Even where consumers do not submit complaints directly to the payment processor, the payment processor can access complaints online through databases such as the Better Business Bureau.

In CFPB v. Global Client Solutions, the CFPB alleged that a third-party payment processor was liable under the Consumer Financial Protection Act (CFPA) for processing payments on behalf of unlawful debt relief service providers when the payment processor received hundreds of complaints from consumers. In Reyes, the plaintiffs sufficiently pled that a third-party payment processor knew that its clients were engaged in fraudulent telemarketing in part because the payment processor had received complaints from at least one consumer. Similarly, where a third-party payment processor receives com-

---

162. Id.
163. See Letter from Justin E. Kolber to Marsha Jones, supra note 61.
165. See FDIC FINANCIAL INSTITUTION LETTER, supra note 36, at 3.
plaints about its lender clients, that should help establish that the payment processor had actual knowledge of the merchant’s wrongdoing.

Another particularly inculpatory red flag is the high return rate of ACH debit transactions.169 A “return rate” is the frequency with which an ACH debit cannot be completed170 because the attempted debit is refused by the consumer’s bank.171 “In the banking and payment processing industries, the monitoring of merchant return rates is a well-established component of ‘risk management’ practices.”172 Each return is labeled with a reason for the return, which may be indicative of specific forms of wrongdoing by the lender.173 Reasons for return include insufficient funds in the consumer’s account (NSF),174 account number discrepancies,175 and consumer complaints.176

A return rate generated by a lender that is significantly higher than the industry average “should cause a legitimate payment processor to spring into action,”177 or, “at a bare minimum,” trigger “scrutiny and investigation of the merchant’s underlying business practices.”178 In FTC v. Landmark Clearing, Inc., the FTC alleged that because of exceptionally high return rates (some as high as 80%), the payment processor knew, or should have known, that the consumers had not validly authorized the debits.179 In the face of a high return rate, especially where the returns are generated by highly suspicious circumstances such as consumer complaints, the payment processor likely knows that the lender is engaged in an unlawful or abusive practice.

Where a third-party payment processor is on notice of its lender client’s wrongdoing by way of the merchant application, a monitoring system, red flags, or both, consumer plaintiffs may sufficiently establish that the payment processor had the actual knowledge required for aiding and abetting liability.

b. Substantial Assistance. In addition to establishing actual knowledge, to state a claim for aiding and abetting liability consumer plaintiffs must establish that the third-party payment processor provided the lender with substantial

169. See, e.g., Complaint, Hillick v. BMO Harris Bank, supra note 32, at ¶ 66; FDIC FINANCIAL INSTITUTION LETTER, supra note 36, at 5; Bernardo, et al., supra note 144; FTC Press Release, supra note 23.
171. See 16 C.F.R. § 310 (2015); see also Complaint, FTC v. Landmark Clearing, Inc., supra note 23, at ¶ 34.
173. See id.
174. See id.
175. See id.
179. See id. at ¶ 29 (alleging that return rates of 50%, 70%, and 80% were “obvious” indications that there was either no consumer authorization or that the consumer’s authorization was based on deceptive information).
assistance. Plaintiffs can sufficiently plead the substantial assistance element of aiding and abetting by alleging that the payment processor engaged in ordinary business transactions on behalf of the lender, gave an aura of credibility to the lender, or enabled the lender to access funds.

In *In re First Alliance Mortgage Co.*, the court explained that a bank’s ordinary business transactions performed on behalf of a customer can satisfy the aiding and abetting requirement of substantial assistance where the bank “actually knew those transactions were assisting the [primary tortfeasor] in committing a specific tort.” The court expounded, “where a company’s whole business is built like a house of cards on a fraudulent enterprise,” the difference between an ordinary business transaction and substantial assistance “is a distinction without a difference.” The *First Alliance* court’s analysis of a bank’s ordinary business activity as substantial assistance can be applied to a third-party payment processor’s transactions. By initiating transactions and transferring funds on behalf of a lender client, the payment processor engages in ordinary business transactions sufficient to satisfy the substantial assistance element of an aiding and abetting claim.

In *Schulz v. Neovi Data Corp.*, the plaintiff alleged that a third-party payment processor gave the operator of an illegal lottery an “aura of respectability” that “further encourage[d] participation” by the injured parties by providing its name and logo. Where the lender’s clients see a payment processor’s logo, name, or description of services associated with the lender, they may be more likely to contract to borrow from the lender—the payment processor substantially assists the lender by helping to secure consumers to contract with the lenders.

A third-party payment processor may substantially assist unlawful or abusive activity by enabling the lender to obtain access to consumer funds. By enabling the lenders to access client funds, a payment processor makes it possible for the merchant to complete its unlawful and predatory acts such as charging illegal fees. The third-party payment processor “plays a critical role

---


181. 471 F.3d at 995; see also Plaintiff’s Memorandum in Opposition to Gateway’s Motion to Dismiss, Ray v. BlueHippo Funding, *supra* note 131, at *6.


in its client merchants’ unlawful business practices” because “[i]t provides its client merchants with access to the United States banking system, controls the procedures through which money is debited from consumers’ bank accounts, and disburses consumer funds back to its client merchants.”

Third-party payment processors enable merchants to access accounts in states where the merchant’s activity is banned by that state’s law. In *Newton v. American Debt Services*, the court found sufficient evidence, under an aiding and abetting claim against a third-party payment processor, to infer that a payment processor had provided substantial assistance to unlawful debt settlement companies. The court emphasized that without the third-party payment processor’s provision and management of custodial bank accounts, the merchants could not offer debt settlement services. Similarly, where out-of-state lenders contract with consumers in states where their lending is prohibited or effectively banned, the lenders could not access accounts in those states without a third-party payment processor providing them with access to the ACH network. In *Hillick v. BMO Harris Bank*, the complaint alleged that the bank “aided and abetted the Out-of-State Payday Lenders’ violations of New York civil usury law by providing the necessary access to the ACH Network to carry out the Out-Of-State Payday Lenders’ illegal scheme,” and “knowingly provided substantial assistance to . . . the illegal lending activities of the Out-Of-State Payday Lenders.”

**B. NEGLIGENT INFILCTION OF ECONOMIC LOSS**

This section proposes that an alternative theory under which an aggrieved class of borrowers might recover against a third-party payment processor is negligent infliction of economic loss. With a significant amount of information about their lender clients and many ways to learn about their lender clients’ wrongdoing, payment processors are in a strong position to detect and prevent harm to borrowers, and may have a duty to do so. Specifically, this section will (1) explain the doctrine of negligent infliction of economic loss, (2) explore how
it might be applied to third-party payment processors, and (3) argue for extending the doctrine despite its currently limited use. This section concludes that, if availability of the doctrine of negligent infliction of economic loss is expanded, consumers can establish that a payment processor had the actual knowledge required to establish a duty of care via the merchant application, monitoring systems, red flags, and suggestions from institutions to implement risk assessment measures. It further concludes that consumers can show that a payment processor breached that duty of care by continuing to process payments despite knowledge of the lender’s wrongdoing.

1. Doctrine

While courts traditionally do not permit plaintiffs to recover for purely economic loss, some courts have carved out exceptions to that general rule.

a. General Rule Against Recovery. Generally, a purely economic loss cannot be recovered under American tort negligence law. Instead, economic losses are limited to recovery in negligence where there is an additional loss or harm, such as a physical injury. The term “pure economic loss” refers to loss sustained by a plaintiff who has not suffered an injury or damage to tangible property, but has lost funds or value in their property as the result of another’s harm. Although American law generally disfavors recovery for pure economic loss under a theory of negligence, there are exceptions to that general rule.

b. Exceptions. Despite the traditional rule barring recovery of purely economic loss in a negligence action, some courts have been willing to permit such recovery under certain circumstances.

In People Express, the Supreme Court of New Jersey permitted a plaintiff airline to recover for pure economic loss in negligence when the airline lost profits after having to evacuate its offices due to a tank car accident at a nearby

---

190. See, e.g., Robins Dry Dock & Repair Co. v. Flint, 275 U.S. 303, 308 (1927) (reaffirming the rule against recovery for pure economic loss); People Express Airlines v. Consol. Rail Corp., 495 A.2d 107, 109 (N.J. 1985); Herbert Bernstein, Civil Liability for Purely Economic Loss Under American Tort Law, 46 AM. J. COMP. L. 111, 111 (1998) (“In the most general of terms, it can be said that purely economic loss is not recoverable under American tort law rules of negligence.”).

191. People Express Airlines, 495 A.2d at 109 (“It is well-accepted that a defendant who negligently injures a plaintiff or his property may be liable for all proximately caused harm, including economic losses.”); see also Bernstein, supra note 190.


193. Bernstein, supra note 190, at 112; See Powers & Niver, supra note 192, at 481 (“The ‘economic loss’ rule is itself controversial, and some courts have relaxed it in limited circumstances.”).

194. These cases generally fall into three categories: (1) intellectual services, (2) defective products, and (3) interference with the use of resources. Bernstein, supra note 190, at 114–25.
railroad. Rather than require physical harm to find liability for negligence, the court determined that foreseeability was an adequate test, requiring the plaintiff to show foreseeability to establish a duty owed and proximate causation between the breach of duty and the loss. The court explained that a defendant owes a duty of care to take reasonable measures to avoid the risk of causing economic damages, aside from physical injury, to... plaintiffs comprising an identifiable class with respect to whom [the] defendant knows or has reason to know are likely to suffer such damages from its conduct.

The California courts have been particularly willing to impose liability on a defendant that caused a plaintiff to suffer purely economic loss, taking into account the facts of each case. In Union Oil v. Oppen, the Ninth Circuit seemed willing to make policy-based exceptions to the general bar against recovery for pure economic loss in negligence in a case where commercial fishermen sought recovery for loss of profits sustained from an oil spill the defendants had caused while drilling. The Union Oil court, like the court in People Express, found that the presence of a duty owed by the defendants would turn on foreseeability.

In J'Aire Corp. v. Gregory, the Supreme Court of California permitted plaintiff restaurant owners to recover for loss of profits when the lessee's contractor delayed in making improvements to the property. The court emphasized the role of duty of care and reiterated that in California, recovery in negligence may be permitted even where the only harm is economic in nature. The J'Aire court then established six factors for courts to consider when determining whether there was a duty to act reasonably to prevent economic harm:

1. the extent to which the transaction was intended to affect the plaintiff,
2. the foreseeability of harm to the plaintiff,
3. the degree of certainty that the plaintiff suffered injury,
4. the closeness of the connection between the defendant’s conduct and the injury suffered,
5. the moral blame attached to the defendant’s conduct, and
6. the policy of preventing future harm.

At least one California court has already applied the doctrine in the context of third-party payment processors. In Marsh v. Zaazoom, a California district court found that a class of plaintiffs had sufficiently alleged a duty of care owed by

195. See People Express Airlines, 495 A.2d at 114.
196. See id. at 115.
197. Id. at 116.
198. See Union Oil v. Oppen, 501 F.2d 558, 563–65 (9th Cir. 1974).
199. Id. at 566.
200. 598 P.2d 60, 63–64 (Cal. 1979).
201. Id.
202. Id at 63.
third-party payment processors in light of the payment processors’ activities relating to an alleged Internet scam and that they had sufficiently stated a claim for negligence. The consumers alleged that the payment processors’ duty of care arose from creating and depositing checks drawn on the consumers’ accounts. The plaintiffs asserted that the payment processors subsequently breached their duty because they processed payments despite being on notice, based on the “extremely suspicious circumstances surrounding the checks,” that the checks were unauthorized and that they knew or should have known of their merchant clients’ wrongful conduct due to the high return rate, significant number of consumer complaints, inquiries from government agencies regarding the merchant clients, and “peculiarities” on the face of the checks.

2. Application to Third-Party Payment Processors

Aggrieved consumers could attempt to bring a negligence action against their lender’s third-party payment processor. Consumer plaintiffs could establish that the payment processor had the actual knowledge required to establish a duty of care under a negligence cause of action by way of the merchant application, monitoring systems, red flags, and suggestions from institutions to implement risk-assessment measures. Consumer plaintiffs could then establish that the payment processor breached that duty of care by continuing to process payments despite knowing of the lenders’ wrongdoing.

a. Elements. To bring an action for negligence against a third-party payment processor processing payments on behalf of predatory, abusive, or unlawful lenders, the plaintiffs must show that (1) the payment processor had a duty to use reasonable care to prevent reasonably foreseeable economic injury and (2) that the payment processor’s failure to do so was the proximate cause of the consumer’s economic loss. Where a third-party payment processor breaches a duty of care to avoid injury to a “particularly foreseeable plaintiff[],” the payment processor “may be held liable for actual economic losses that are proximately caused by its breach of duty.”

---

204. Id.
205. Id. at *4.
206. Id. at *3–4.
207. Id. at *3.
208. See id. at *2. The court permitted the negligence claim to go forward even though there was neither a contract between the payment processor and the plaintiffs, nor a statute that would create a duty between the payment processor and the plaintiffs. Id. at *20.
209. See Plaintiff’s Memorandum in Opposition to Gateway’s Motion to Dismiss, Ray v. BlueHippo Funding, supra note 131, at *3, *8 (alleging Gateway was liable under a theory of negligence because of a duty to use reasonable care and to prevent reasonably foreseeable economic injury, and proximate causation of the economic loss).
b. Duty. Generally, there is little formal duty imposed upon third-party payment processors. Third-party payment processors are generally self-regulated211 and do not have the same formal duties imposed on them that banks do.212 For example, unlike banks, third-party payment processors generally are not required to have “Know Your Customer” protocols in place.213 Payment processors are also not covered by the Bank Secrecy Act or anti-money laundering laws; therefore, they “are not required to have customer identification programs, conduct customer due diligence, engage in suspicious activity monitoring, or report suspicious activity to federal authorities.”214 Furthermore, third-party payment processors usually are not considered “money transmitters” within the federal definition. Accordingly, they are not required to follow the Money Services Business Guidelines, such as registering with the FinCEN and complying with the BSA.215 The information that a third-party payment processor has by way of the merchant application, monitoring systems, and red flags, in addition to institutional guidance, however, may impose a duty upon them to prevent economic injury to consumers contracting with abusive, predatory, or unlawful lenders.

Many of the same aspects of the lender–processor relationship that may establish actual knowledge under a theory of aiding and abetting may also impose a duty of care on the third-party payment processor under a theory of negligent infliction of economic loss. The information learned through the merchant application and monitoring systems might both establish actual knowledge and create a duty of care. In addition, the recommendations of various institutions and the increased regulatory focus on third-party payment processors may help establish a duty of care.

i. Merchant Application. As discussed in section II.A.3, a third-party payment processor can find initial indications of the lender client’s unlawful or abusive practices by reviewing the lender’s application.216 Similar to how that

211. Jeri Leigh McDowell, Comment, Insidious Design or Instrument of Progress: The Multi-Agency Initiative to Choke Off Undesirable Business’ Access to the Financial World, 47 T EX. TECH. L. REV. 803, 837 (2015); see also Guilty Until Proven Innocent?, supra note 185, at 2 (statement of Scott Talbott, Senior Vice President of Government Affairs, The Electronic Transactions Association); CNAVAZOS-WRIGHT, supra note 92, at 16. Talbott explains that imposing liability on payment processors for their customers’ wrongdoing increases the cost of doing business for payment processors. See Guilty Until Proven Innocent?, supra note 185, at 2. This increased cost in turn lowers the payment processors’ risk tolerance, leading them to deny payment processing services to entire categories of legitimate, but slightly riskier, merchants, such as start-ups with little credit history. Id.

212. See, e.g., CNAVAZOS-WRIGHT, supra note 92, at 16 (explaining that third-party payment processors, unlike banks, are not required to implement “Know Your Customer programs”).

213. Id.


216. See supra Section II.A.3.a.i.
information may provide the payment processor with actual knowledge under a
theory of aiding and abetting, it may also put the payment processor on notice
of wrongdoing and create a duty of care under a theory of negligent infliction of
economic loss. For example, in Landmark Clearing, the FTC alleged that a
third-party payment processor was “on notice” that its merchant client “would be engaging in unauthorized debiting” because of the information contained in
the merchant application.217

With the information contained in the lender’s application, a third-party
payment processor can run a basic review of the lender’s history to determine if
the lender has been involved in any prior civil, criminal, or regulatory investiga-
tions or actions.218 Where the lender has been involved in such actions, that
information gives the payment processor reason to be suspicious and may create
a duty of care by the payment processor to ensure that similar unlawful acts are
not taken against the lender’s current clients.

From the lender client’s application, the third-party payment processor may
determine the lender’s client base. The makeup of a lender’s client base is a
widely known risk factor.219 Where the payment processor can deduce a
lender’s general client base, an even stronger argument can be made that the
consumers are “particularly foreseeable plaintiffs” to whom the payment proces-
sor owes a duty because they are an even smaller, more specific group of
consumers and known to be the target of unlawful lender activity.

The merchant application may also notify the third-party payment processor
of certain characteristics of a lender’s business that may put the third-party
payment processor on notice of the lender’s questionable activity.220 For ex-
ample, the characteristics of out-of-state payday lenders put a third-party pay-
ment processor on notice that a lender’s borrowers are the victims of unlawful
activity.221 In this scenario, consumers in states where payday loans are prohib-
ited may be classified as “particularly foreseeable plaintiffs.” 222

218. Bernardo et al., supra note 144.
219. See FDIC FINANCIAL INSTITUTION LETTER, supra note 36, at 1 (explaining that payment proces-
sors for telemarketers and online merchants tend to have a higher risk profile, as those clients “tend[] to
display a higher incidence of consumer fraud or potentially illegal activities than some other
businesses”).
220. See supra Section II.A.3.a.i. For example, online merchants tend to pose a higher risk of fraud
and illegal activity. See generally FDIC FINANCIAL INSTITUTION LETTER, supra note 36; FinCEN, supra
note 81.
221. See NYDFS Press Release, supra note 148 (explaining finding that many out of state lenders
“use the Internet to solicit and provide illegal payday loans” where they are prohibited); Complaint,
Hillick v. BMO Harris Bank, supra note 32, at 21 (explaining that the characteristics of out-of-state
payday lenders put ODFIs on notice of their unlawful activity). In Hillick, the plaintiffs alleged that a
defendant bank that initiated entries on the ACH network for a lender knew that the lender was an
out-of-state payday lender. Id. at 20–21, 29.
222. People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d, 107, 118 (N.J. 1985). One line of
exceptions to the general bar against recovery for purely economic loss is situations where the plaintiff
can show that the defendant knew that his negligence would cause economic loss to a particularly
foreseeable plaintiff. Id. at 112.
From the application, the third-party payment processor may determine that the merchant was referred by an ISO. A third-party payment processor may contract over time with the same ISO for merchant referrals. If that ISO has referred predatory lenders to that third-party payment processor in the past, it should be suspicious of a subsequent referral by that ISO.223

In addition to reviewing the application, a payment processor can, at the outset, learn about a lender client’s unlawful or abusive practices by running a verification check on the lender’s business. By comparing the information in the application with public records and fraud databases, or by comparing the information to that held by third parties, such as consumer reporting agencies, the payment processor can determine whether the lender is running a legitimate or illegitimate business.224

ii. Monitoring Systems. Like the way in which monitoring systems may establish actual knowledge under a theory of aiding and abetting,225 they may also impose a duty of care on third-party payment processors under a theory of negligent infliction of economic loss. Monitoring systems, voluntary226 or through an agreement with a bank,227 may put payment processors on notice that a lender’s clients are at risk of economic loss. In FTC v. InterBill, Ltd., the FTC alleged that InterBill, a third-party payment processor, should have known that its client was involved in a fraudulent operation, but failed to detect numerous red flags because it did not follow its own vetting and monitoring protocol.228 In Universal Debt & Payment Solutions, the CFPB alleged that third-party payment processors working on behalf of unlawful phantom debt collectors acted “knowingly” and “recklessly” where they “ignored their own stated policies concerning whether to approve the debt collectors’ applications.”229 Where a third-party payment processor contracts with its bank to undertake certain due diligence procedures, it may be required to monitor for suspicious activity, such as high return rates.230 These procedures may impose a duty of care on the payment processor either by creating an expectation in consumers that the third-party payment processor is protecting them from

223. See supra Section II.A.3.a.i.
224. See OCC BULLETIN 2008–2012, supra note 141 (suggesting that banks verify the legitimacy of a merchant’s business through these techniques).
225. See supra Section II.A.3.a.ii.
226. See Witkowski, supra note 183 (describing CPFB complaint against payment processors for unlawful debt collectors who had monitoring systems in place capable of discovering the alleged unlawful activity, but who failed to use those systems to stop the fraudulent activity).
227. See Complaint, CFPB v. Universal Debt & Payment Solutions, LLC, supra note 151, at ¶ 80 (in suing third-party payment processor involved in phantom debt collection scheme, CFPB alleged that the payment processor had contracted with its bank to monitor chargebacks, and that it had failed to investigate suspicious activity on the debt collectors’ accounts).
228. Complaint, FTC v. InterBill, Ltd., supra note 157, at ¶¶ 15–16.
229. See Kaufman & Fioccola, supra note 158; see also Complaint, CFPB v. Universal Debt & Payment Solutions, LLC, supra note 151, at ¶ 329.
230. See Complaint, CFPB v. Universal Debt & Payment Solutions, LLC, supra note 151, at ¶ 80.
suspicious activity, or by alerting the payment processor to activity that would put it on notice of potential harm to consumers.

iii. Red Flags. As discussed in section II.A.3, throughout the processing relationship, third-party payment processors may become aware of “red flags” that indicate that their lender clients are engaged in unlawful or abusive practices. Such red flags may include consumer complaints against the lender, a high return rate, and prior legal or regulatory actions against the lender.

Consumer complaints can help establish actual knowledge for aiding and abetting; they can similarly create a duty of care. Where a third-party payment processor receives consumer complaints regarding its lender clients, the payment processor has reason to suspect that the lender is engaged in suspicious activity and that the lender’s clients are incurring harm, supporting a finding of a duty owed by the payment processor.

Another particularly telling red flag that can establish both actual knowledge and a duty of care is a high return rate. In *Landmark Clearing*, the FTC alleged that because of exceptionally high return rates, the third-party payment processor “knew, or should have known,” that the consumers had not validly authorized the debits. A high return rate should raise the payment processor’s suspicions that the lender’s consumers are the victims of abusive or unlawful practices and “set off alarm bells.” Accordingly, the lender’s clients are particularly foreseeable plaintiffs, creating a duty on the payment processor to protect them from further harm.

In addition, where a lender has been the subject of prior civil, criminal, or regulatory actions, a duty owed by the third-party payment processor to the consumers may arise. Because the lender is known to have engaged in unlawful acts in the past, the payment processor can reasonably foresee that it may

---

231. See supra Section II.A.3.a.iii.
232. See id. In *Global Client Solutions*, the CFPB alleged that a payment processor was liable under the CFPA for processing payments on behalf of unlawful debt relief service providers when the payment processor received hundreds of complaints from consumers. Complaint at ¶ 20, CFPB v. Global Client Solutions, No. 2:14-cv-06643, 2014 WL4243266 (C.D. Cal. Aug. 25, 2014). In *Reyes*, the plaintiffs sufficiently pled that a payment processor knew that its clients were engaged in fraudulent telemarketing, in part because the processor had received complaints from clients. *Reyes* v. Zion First Nat’l Bank, No. 10-345, 2012 WL 947139, at *3 (E.D. Pa. Mar. 21, 2012).
233. See supra Section II.A.3.a.iii; see also Complaint, Hillick v. BMO Harris Bank, supra note 32, at 21; *FDIC Financial Institution Letter*, supra note 36, at 5; Bernardo et al., supra note 144; FTC Press Release, supra note 23.
235. See id. (arguing that a higher than average return rate is an indicator of unauthorized debiting); *see also* *FDIC Financial Institution Letter*, supra note 36, at 5 (“[H]igh rates of return may be an indicator of unauthorized or illegal activity.”).
236. Fair, supra note 177.
engage in similar practices in the future, and that the consumers may subsequently suffer loss just as the lender’s prior victims did.

iv. Institutional Recommendations. Various entities have suggested that third-party payment processors should have risk assessment measures in place that would alert them to unlawful or abusive activity by lender clients. These recommendations bolster the argument that the payment processors have a duty to prevent economic injury to consumers. For example, the FDIC suggested that third-party payment processors should “have effective processes for verifying their merchant clients’ identities and reviewing their business practices.” In addition, the Vermont Attorney General has written letters to various entities asking that they urge third-party payment processors to undertake due diligence procedures. For example, in a letter to the Third Party Payment Processors Association, the Vermont Attorney General’s Office requested help in combating illegal and predatory lending. In a similar letter to NACHA, the Attorney General’s Office suggested that NACHA counsel third-party payment processors to take active steps to guard against unauthorized loan transactions. The fact that a state Attorney General’s Office is advocating for due diligence measures by third-party payment processors, especially if the requests are heeded and the TPPPA and NACHA advise payment processors on the topic, supports imposing a duty on payment processors to take reasonable care to prevent economic injury to consumers of short-term loans.

Another way that a duty of care might be imposed on third-party payment processors is through the recent increase in regulatory focus on payment processors. Recently, “[t]he short-term lending industry has increasingly become the subject of government investigations and enforcement actions at both the federal and state levels.” In the past few years, the attention has broadened to third parties in the short-term lending industry, including third-party payment processors. For example, the CFPB sued third-party payment processors for their participation in unlawful debt collection practices, asserting that the payment processors “should have known” about the alleged violations occurring via their processing services. Through Title X of Dodd-Frank the CFPB has the power to sue third-party payment processors for “knowingly or recklessly” providing “substantial assistance” to covered persons (who are, for

237. See Reyes, 2012 WL 947139, at *4–6 (plaintiffs sufficiently pled that a payment processor knew that its clients were engaged in fraudulent telemarketing in part because the telemarketers in question were known to have engaged in similar fraud in the past).

238. FDIC FINANCIAL INSTITUTION LETTER, supra note 36, at 1.

239. Letter from Justin E. Kolber to Marsha Jones, supra note 61, at 1.

240. Letter from Justin E. Kolber to Janet O. Estep, supra note 164, at 1.


242. Id.

243. Witkowski, supra note 183.
our purposes, unlawful lenders). 244 Title X and the CFPB’s prior actions under Title X help create a duty of care on third-party payment processors.

The FTC has also increased its focus on third-party payment processors. In *Landmark Clearing*, the FTC sued third-party payment processors for their role in debiting consumer accounts on behalf of merchant clients despite the existence of high return rates and other red flags. 245 With the increase in regulation of and focus on payment processors by agencies, payment processors should know that they are expected to take reasonable steps to protect consumers, should know the kinds of actions they are expected to take, and should know the type of consumers likely to become victims.

This level of regulation is likely to continue (if not increase), which will put more scrutiny and pressure on third-party payment processors. The longer these enforcement actions continue, and the more aggressively they are brought, the stronger the argument will be that payment processors have a duty to protect the foreseeable class of consumers from economic injury. Already, the “DOJ’s increased pressure and attempts to impose vicarious liability on the payment processing system require payment processors to alter their risk management procedures.” 246 Third-party payment processors are aware that they are being scrutinized and aware that they must act accordingly—with due care.

Third-party payment processors know that their lender clients are offering consumers short-term, high interest loans. 247 Knowledge of who the general class of persons working with their lender clients is, in combination with various red flags that lender clients are engaged in unlawful or abusive business practices, makes the consumers “particularly foreseeable plaintiffs” and imposes a duty upon the payment processors to avoid economic loss to those consumers.

c. Breach of Duty. A third-party payment processor breaches its duty to the consumer where it knew, or should have known, that its lender client is engaged in unlawful or abusive activity, but nonetheless continues to process payments on the lender’s behalf. 248 A third-party payment processor facilitates unlawful activity by enabling the merchants to obtain access to consumer funds when the payment processor knows, or should know, that the merchants are engaged in

245. See Complaint, FTC v. Landmark Clearing, Inc., *supra* note 23, at ¶ 67. In some cases, the payment processor ignored return rates of 50–80%, where the industry average is about 1%. *Saunders et al., supra* note 90, § 3.13.3.
246. McDowell, *supra* note 211, at 832–33.
247. See *Kolber & Morgan, supra* note 22, at 6 (“The processors know their clients are lenders of high-interest internet loans or payday loans.”).
248. See *Witkowski, supra* note 183 (explaining CFPB complaint against payment processors working with “phantom debt” collectors, which asserts that the payment processors should have known that the debt collectors were collecting phantom debts, but continued to do business with the debt collectors anyway, thus becoming liable for the unlawful conduct).
unlawful conduct. In *Universal Debt & Payment Solutions*, an action by the CFPB, the court found that the payment processor had breached a duty of care. The court noted that the payment processor was “highly unreasonable” in ignoring red flags that indicated that the merchant debt collectors were engaged in fraud. The court explained that the third-party payment processor’s decision to ignore the red flags was an “extreme departure from the standards of ordinary care.”

The third-party payment processor is the proximate cause of the harm to the consumer. As the party responsible for transmitting payments from the consumers, the payment processor makes it possible for the lenders to engage in their unlawful or unfair practices. Without the involvement of the third-party payment processors, the consumers would not suffer an economic loss at all.

3. Argument for Extending Exceptions

In light of the limited recognition courts give to the validity of claims for purely economic loss, recovery on a negligence claim may be difficult for plaintiff borrowers. But there is reason to support an extension of the doctrine and permit more plaintiffs, including borrowers harmed by third-party payment processors, to recover for pure economic loss.

Some scholars argue that the denial of recovery for pure economic loss in negligence is hard to reconcile with the availability of recovery for large economic losses resulting from negligently caused physical harm. In *People Express*, the court explained that the many exceptions that have arisen to the traditional bar against recovery for pure economic loss “have... created lasting doubt as to the wisdom of the per se rule of nonrecovery for purely economic losses.”

In addition, the pragmatic arguments proffered for sustaining the rule can be easily undermined. Proponents of the general rule argue that it is necessary to limit recovery and prevent “fraudulent claims, mass litigation, and limitless...
liability, or liability out of proportion to the defendant’s fault."\(^{257}\) Yet, in light of the large recoveries awarded in many of today’s mass tort cases for physically injured plaintiffs, that explanation is weak.\(^{258}\) Further, despite the difficulty of defining damages and the risk of infinite liability in non-physical harm claims for emotional distress and loss of consortium, courts continue to allow recovery in such cases notwithstanding concerns of “widespread liability.”\(^{259}\)

Although the concerns of a wide breadth of liability are valid, “[t]he answer to the allegation of unchecked liability is not the judicial obstruction of a fairly grounded claim for redress. Rather, it must be a more sedulous application of traditional concepts of duty and proximate causation to the facts of each case.”\(^{260}\) Like other areas of negligence law, widespread liability in pure economic loss cases can be limited by narrowing recovery to only certain situations.\(^{261}\) Purely economic losses stemming from unlawful or abusive lending “are borne by innocent victims, who may not be able to absorb their losses.”\(^{262}\) Courts should seek to construct a doctrine that limits liability while permitting legitimate claims against third-party payment processors to go forward,\(^{263}\) allowing victim borrowers to become whole again.

III. VERMONT LAW AS A MODEL FOR OTHER STATES

Holding third-party payment processors liable for the actions of their lender clients in most states may prove difficult; one state, however, has circumvented that difficulty by enacting legislation that provides a direct route to holding third-party payment processors for lenders liable. In 2012, Vermont passed the Vermont Consumer Protection Act (the Vermont Act),\(^{264}\) making Vermont law unique in its ability to police predatory online lending.\(^{265}\) The Vermont Act applies consumer protection laws to both lenders and entities that assist lenders, such as third-party payment processors.\(^{266}\) Vermont’s unique statutory scheme should serve as a model for other states looking to hold third-party payment processors liable for their involvement in unlawful and abusive lending.

---

\(^{257}\) *People Express Airlines*, 495 A.2d at 110; see also *In re Kinsman Transit Co.*, 338 F.2d 821, 823 (2d Cir. 1968).

\(^{258}\) See Bernstein, *supra* note 190, at 126.


\(^{260}\) *People Express Airlines*, 495 A.2d at 111.

\(^{261}\) Rabin, *supra* note 259, at 1527. Rabin would limit liability to situations falling within a category of “triangular configurations,” allowing recovery only for intended beneficiaries. *Id.*

\(^{262}\) *See People Express Airlines*, 495 A.2d at 111.

\(^{263}\) See generally *id.* (describing the policy justifications for extending tort liability to allow recovery for pure economic loss).

\(^{264}\) 8 V.S.A. § 2709 (2016).

\(^{265}\) See Kolber & Morgan, *supra* note 22 at 1 (“In May 2012, the Vermont Legislature enacted the strongest law in the nation on predatory online lending.”).

\(^{266}\) *Id.*
The Vermont Act makes it an “unfair and deceptive act and practice in commerce for a processor . . . to process a check, draft, other form of negotiable instrument, or an electronic funds transfer from a consumer’s financial account in connection with a loan solicited or made by any means to a consumer” in violation of Title 8, chapter 73. Under Title 8, chapter 73, all lenders must be appropriately licensed and may not charge an interest rate greater than 12–24% per annum. Any third-party payment processor that processes payments on behalf of a lender that is in violation of the Vermont Act can itself be held liable.

The Vermont Attorney General’s actions to date against third-party payment processors illustrate how the Vermont Act works and how similar acts would be employed if they were adopted in other states. In October 2014, for example, the Vermont Attorney General’s office settled a claim with Intercept Corporation, a North Dakota-based third-party payment processor. The complaint against Intercept alleged that between 2012 and 2013 it processed debits from more than 1,000 Vermont consumer bank accounts on behalf of high-interest, short-term lenders. The loans that Intercept processed imposed egregious interest rates of over 100–300%, clearly in violation of the 24% maximum rate permitted under the Vermont Act. Pursuant to the settlement, Intercept paid $75,000 to Vermont consumers and $10,000 to the State.

In March 2016, the Vermont Attorney General settled a claim with Advantage, a Nevada-based third-party payment processor. Advantage processed ACH payments on behalf of thirty-six lenders offering high interest, small-dollar loans over the Internet to consumers in Vermont. None of these lenders were licensed to make loans in Vermont, and, therefore, all were operating in violation of the Vermont Act. The Vermont Attorney General’s office alleged that Advantage had engaged in unfair acts and practices in commerce in violation of section 2453 of the Vermont Act by processing transactions from Vermont consumers’ bank accounts on behalf of unlicensed lenders.

Vermont’s success in combatting unlawful and predatory lending within its borders can be mirrored by other states. By enacting consumer protection laws

---

267. 9 V.S.A. § 2481w(c) (2016).
268. 8 V.S.A. § 2201 (2016).
269. 9 V.S.A. § 41a(b)(5) (explaining the maximum interest rate percent per annum that a lender may charge depends on the type of loan).
271. Id.
272. See id.
273. Id.
275. Id.
276. Id.
277. See 8 V.S.A. § 2201.
278. See Verdict and Settlement Summary, Vermont v. Advantage Payment Sys., supra note 274.
like the Vermont Act, other states could hold third-party payment processors that facilitate predatory and illegal lenders responsible for the harms caused by abusive and illegal loans.

CONCLUSION

Every year millions of Americans fall victim to predatory, abusive, and unlawful practices of short-term lenders. Unfortunately, many consumers are unable to recover their losses against lenders because of techniques lenders use to evade liability, such as operating online, overseas, through rent-a-bank arrangements, or through Native American tribes. In light of that injustice, the focus has shifted to entities that facilitate short-term lending schemes, including third-party payment processors. To date, few suits have been brought against third-party payment processors despite the critical role that payment processors play in predatory, abusive, and illegal lending schemes.

This Note argued for focusing liability on third-party payment processors to gain redress for consumers unable to recover directly from lenders. This Note suggested that borrowers might be able to seek redress by alleging that a payment processor is liable under a theory of aiding and abetting. Additionally, this Note proposed that consumers might be able to recover under a theory of negligent infliction of economic loss. Still, such suits may prove difficult. Finally, as an alternative way to protect consumers from falling victim to the acts of lenders and their third-party payment processors in the future, this Note suggested that states might consider adopting legislation that holds third-party payment processors directly liable for violations of consumer protection laws.