Emerging Technologies

In Pursuit of Consumers—Merchant Payments via Contextual Commerce

Sean Ruff and Crystal Kaldjob

Emerging payment technologies are changing the way in which merchants and the financial services industry operate. The introduction of new business models, new players entering the financial services space, and new and innovative methods of customer service have all significantly impacted one of the most important interactions between merchants and customers—payments.

Against this backdrop, this chapter addresses the concept of “contextual commerce” as a private-label vehicle for merchants to target both existing and potential customers outside of traditional merchant e-commerce channels, including social media platforms and other web-based consumer gathering points. In doing so, this chapter discusses some of the key legal and regulatory considerations that govern the application of these types of payment transactions, including the use of digital wallets and stored value. While it is beyond the scope of this chapter to cover all legal and regulatory issues that may impact payments facilitated via contextual commerce, those legal and regulatory issues identified represent a collection of the most interesting and, in some cases, difficult applications of current law.

Sean Ruff is of counsel in the Financial Services Practice Group of Morrison & Foerster LLP and co-chair of the firm’s Fintech Practice Group. Crystal Kaldjob is an associate in the Financial Services Practice Group of Morrison & Foerster LLP.
I. INTRODUCTION

The technological capability of smartphones and other portable electronic devices that can access the Internet has increased dramatically. These capabilities have taken advantage of improvements in communication enabled by mobile phones and mobile “apps” and combined them with existing payment platforms, thus facilitating more efficient payment communications between the payment parties (e.g., merchants and holders of debit cards and credit cards). This enhanced functionality has led to the development of new ways for consumers to engage in traditional financial services transactions, which have transformed the payments industry by establishing new channels through which merchants can seamlessly interact with consumers.

The notion that merchants can enable consumers to execute purchase transactions via channels not typically associated with a merchant’s physical or virtual location is not new. But as much as the smartphone and other electronic portable devices have changed the face of payments, so too have these devices changed the way consumers lead their lives. For example, the proportion of online time Americans spend on their mobile devices increased from 12.7 percent in 2008 to 54.6 percent in 2015. As smartphones become more prevalent, users tend to access their social networks more on their mobile devices. At the end of 2013, 98 percent of time spent on Instagram was via mobile device, 92 percent for Pinterest, 86 percent for Twitter, and 68 percent for Facebook. As more of a consumer’s time is spread among an ever-growing number of social media platforms, merchants find it necessary to interact with consumers in these consumer-dictated contexts, as opposed to merchant-defined contexts.

This concept of dealing with a consumer on the consumer’s own terms is sometimes referred to as “contextual commerce,” which embodies the idea that consumers can make purchases seamlessly inside the environments that they use regularly.
for other reasons. The idea that, with the touch of a button, consumers could buy anything, anywhere, at any time was the impetus behind the effort of several high-profile social media platforms to operationalize contextual commerce.

For example, in September 2014, Twitter began the rollout of its “buy button” technology, which allowed a consumer to purchase a product directly from a tweet. With the initial rollout of the buy button, a small percentage of U.S. users would see a buy button on tweets from Twitter’s test partners. After hitting the Twitter buy button, customers received additional product details and then could enter shipping and payment information. By September 2015, Twitter joined with several e-commerce platforms to make it easier for merchants to sell products with buy-button tweets.

Pinterest followed Twitter with the launch of its buy-button technology in mid-2015. Prior to launching the Pinterest buy button, users interested in buying an item would be directed to the retailer’s website, where the user would have to search for the item again. The Pinterest buy button launched with several large retailer partners, including Macy’s, Nordstrom, and Neiman Marcus. When purchasing with the Pinterest buy button, users were able to scroll through different views of a product and select product colors. The Pinterest buy button allowed checkout using a credit card.

Instagram launched its buy-button technology in November 2016, with just 20 retail partners. With Instagram’s buy button, when one of the partner brands posts a picture on Instagram, users can tap a button to make prices appear for up to five pictured items. A user can then tap one of the items to shop for it on the brand’s website through Instagram’s in-app browser. Facebook first started testing

---

10. Id.
11. Id.
14. Id.
15. Id.
18. Id.
19. Id.
20. Id.
buy buttons on users’ news feed pages, posts, and ads in 2014. More recently, Facebook launched technology that facilitates a merchant’s ability to add a buy button to artificial intelligence (AI) bot interactions with a consumer through the Messenger app.

Each of these implementations was an effort to reach consumers more effectively to turn “social engagements” into sales. With nearly 80 percent of the U.S. population using social media, and with this percentage expected to increase each year, buy-button technology can link customers within social media apps to merchants, and thereby enable merchants to reach these customers.

Despite the advantages of contextual commerce in targeting interested consumers, the friction caused by the underlying payment function may continue to present barriers to consumer acceptance. While transaction friction is an issue that has beleaguered online payments generally, it appears that it may play a significant role in the consumer failure to embrace buy-button and other related technology meant to facilitate contextual commerce. For example, contextual commerce solutions that effectively target consumers, but then redirect the consumer back to the merchant’s own website to complete a purchase transaction, have seen reduced conversion rates. Add to the process an inefficient payments flow, such as a consumer having to key in various pieces of information such as user name, password, or billing information, and the rate of transaction abandonment increases significantly.

Given such challenges, potential solutions are beginning to appear. For example, ride-sharing platforms such as Uber have attempted to address the issue of

---

23. See Gonçalves & Raatikainen, supra note 8.
27. Karen Webster, What’s More Valuable—A Buy Button or a Digital Wallet?, July 13, 2015 (noting the “obvious” limitation of buy buttons—“they can only be used on the site that is enabling it”), http://www.pymnts.com/news/2015/whats-more-valuable-a-buy-button-or-a-digital-wallet/.
28. Ashwin Shirvaikar, Contextual Commerce, in Disruptive Innovations IV: Ten More Things to Stop and Think About 22 (Citi 2016), available at https://ir.citi.com/TRk1lgLXY1sehGYbkjzU8ZK8ajrDvDG0UxZKC12Cy2nKapNyHQeYkKzeg5c0jdjByk337t%3D.
payments friction by making payment for a transaction all but invisible.\textsuperscript{30} The luxury of being able to exit a car at one’s destination without having to worry about the physical payment transaction cannot be overstated.\textsuperscript{31} And the card-on-file payment process that runs in the background serves as the cloaking device for the physical payment process, without which a quick exit from the car free from fumbling for (or worrying about) a payment method would be impossible.\textsuperscript{32}

While centrally stored payment credentials within a digital wallet (or similar device) may alleviate at least some of the friction that can arise in contextual payments transactions, other solutions such as centralized stored-balance accounts have the potential of addressing the issue as well.\textsuperscript{33} Nevertheless, facilitating a true “one button” contextual payments solution in which consumers can seamlessly pay for goods and services across many different digital platforms without having to visit other websites or provide substantial additional information to complete the transaction will require collaboration and partnership across many entities, including merchants, payment processors, and digital platforms.\textsuperscript{34}

As with most issues concerning financial services, the legal framework upon which contextual commerce payments are built is complex, including a mix of federal and state laws and regulations. While other chapters in this book address these laws and regulations in greater detail, the remainder of this chapter will provide an overview of some of the most important legal and regulatory issues that face participants in this area, with an emphasis on laws that may provide the greatest functional hurdle for participants in contextual commerce payments. These include state money transmission laws and the prospect of state money transmitter licensing; federal Bank Secrecy Act (BSA) compliance; federal laws aimed at services that provide stored value; as well as nonlegal frameworks, such as the Payment Card Industry Data Security Standards (PCI DSS), and the implications of that framework for contextual commerce stakeholders.

\textsuperscript{31} See id. (noting that “Uber is a godsend” because it is so “frictionless”; “when you are done with your ride, you just get out of the car”).
\textsuperscript{34} Andrew B. Morris, Why Context Matters in Commerce, N>GENUITY J., Oct. 18, 2016 (noting that “there is greater need for collaboration and partnership, often between payments industry competitors, as the commerce ecosystem becomes increasingly integrated and complex”), http://tsys.com/ngenuity-journal/why-context-matters-in-commerce.html.
II. KEY LEGAL AND REGULATORY ISSUES

A. State Money Transmission Laws/Federal BSA

1. State Money Transmission Laws

Almost all U.S. states require nonbank entities engaging in the business of money transmission to be licensed.35 There are a variety of actions that can trigger state money transmission licensing and compliance obligations, including receiving and transmitting money, selling or issuing payment instruments or money orders, providing bill payment services, issuing or selling stored value, etc.36 With respect to facilitating contextual commerce payments, however, there are two primary licensing triggers: the receipt and transmittal of funds, and the issuance of open-loop stored value.

a. Receipt and Transmittal of Funds

State money transmitter laws generally define money transmission to include “receiving” money for transmission.37 While this definition is broad, the “classic” money transmission model is a service in which an entity receives funds from a sender and makes a promise to that sender to deliver the funds to another party, on the sender’s behalf.38 In this scenario, the transmitting entity is acting as an “agent” of the sender who holds funds in trust for the sender in the course of transmitting those funds consistent with the sender’s instructions. State money transmission licensing laws, with their emphasis on safety and soundness, are often interpreted as seeking to protect the sender of funds by ensuring that when an intermediary (i.e., a money transmitter) receives those funds, it will deliver the funds as promised (and have funds available to do so). Nevertheless, in some cases, regulators have suggested that even if an entity does not physically control funds (i.e., actually receive the funds), the entity may still be subject to regulation as a money transmitter if it has “constructive control” of the funds.39

35. See, e.g., Fla. Stat. § 560.125(1) (requiring a license to engage in the business of a money services business); 205 Ill. Comp. Stat. 657/10 (requiring a license to engage in the business of transmitting money); Md. Code Ann., Fin. Inst. § 12-405(a) (requiring a license to engage in the business of money transmission).

36. See, e.g., Md. Code Ann., Fin. Inst. § 12-401(m) (defining money transmission to include “selling or issuing payment instruments or stored value devices, or receiving money or monetary value . . .” and including bill payment services).


38. Only a few states explicitly exempt business-to-business funds transfers. See, e.g., N.C. Gen. Stat. § 53-208.42(12) (defining money transmission to involve activity “primarily for personal, family, or household purposes”). Most states interpret their money transmission laws to apply to the transmission of funds on behalf of businesses as well.

Ultimately, however, nonbank entities not otherwise exempt from state money transmitter licensing that facilitate contextual commerce payments by receiving funds for transmission to the merchant may be subject to state money transmitter laws. As the entity processing payments on behalf of merchants, and typically (but not always) receiving settlement funds prior to settling such funds to the merchant in the context of contextual commerce payments transactions, nonbank payment processors, including payment facilitators (and any other nonbank entity performing similar activities) should be aware of these laws and licensing requirements and assess potential applicability.

However, in the context of “payment processing,” based on the specific activity of the nonbank payment processor (or an entity acting in a substantially similar manner to a payment processor), state-by-state exemptions to money transmitter licensing and compliance requirements may be available on a fact-specific, case-by-case basis. Because nonbank payment processors typically (but not always) act on behalf of the ultimate recipient of the funds (i.e., the merchant), as opposed to providing a service to a sender of funds, a nonbank payment processor may not be subject to certain state money transmission laws by its actions as an agent of the recipient of transaction funds, or, in other words, its role as an “agent of the payee.” Under this theory, when the payment processor receives the funds, it is as if the funds have been received, as a matter of agency law, by the ultimate recipient. Based on this interpretation, it follows that there is no “transmission” to another party, nor is there a promise made to any sender to make funds available at another location or to another party.40

Nevertheless, state money transmission regulators have struggled with how to treat “payment processor” and “agent of the payee” transactions. While many state regulators have not taken a formal position on whether their state law governs “agent of the payee” transactions, some states have determined in recent years that “payment processors” acting as “agents of the payee” are not money transmitters41

40. See, e.g., Texas Department of Banking, Op. No. 14-01 (May 9, 2014) (observing that when the “agent” receives the funds, “it is the Biller receiving the funds. . . . In essence, the agency relationship renders the exchange a two-party transaction between the Biller and the customer. Without receipt of money in exchange for a promise to make it available at a later time or different location, there is no money transmission.”); Illinois Department of Financial and Professional Regulation, Statement Regarding Third-Party Payment Processors and the Transmitter of Money Act (observing that “due to the contractual relationship with the third-party payment processor, the merchant will always have a method to address any issues with the third-party payment processor” and reasoning that because the third-party processor is acting as agent for the merchant in accepting and processing funds, “there is no transaction that would fall under the definition of transmitting money” under the Illinois money transmitters law), http://www.idfpr.com/DFI/CCD/pdfs/07292015StatementThirdPartyProcTOMA.pdf.

41. In recent years, states that have established or otherwise indicated by regulation, statutory change, guidance, or other formal communication that an agent of the payee and/or a payment processor is not subject to licensing as a money transmitter include: California, Idaho, Illinois, Kansas, Kentucky, North Carolina, Pennsylvania, Texas, and Virginia. States including Nebraska, Nevada, New York, and Ohio have historically had payee agent exemptions in their money transmitter statutes.
and are exempt from regulation under such states’ money transmitter licensing laws, provided that certain criteria are met.42

The most notable example is California, which exempts from its money transmission law a “transaction in which the recipient of the money or other monetary value is an agent of the payee pursuant to a preexisting written contract and delivery of the money or other monetary value to the agent satisfies the payor’s obligation to the payee.”43

b. Issuance or Sale of Open-Loop Stored Value/Prepaid Access

At the state level, “open-loop” stored value (i.e., may be used with multiple unaffiliated sellers of goods or services) is generally subject to state money transmission licensing and compliance obligations. Specific definitions (as well as the terminology) of stored value (e.g., “closed loop” versus “open loop,” “prepaid access,” etc.) vary under state laws, but the general concept of a covered stored-value product (i.e., an open-loop stored-value product) is money or monetary value evidenced by an electronic record that is prefunded and for which value is reduced on each use—and that is not otherwise exempt as closed-loop stored value.44 Closed-loop products are generally those issued by a merchant that can be redeemed only by that merchant or at a defined set of related merchants.45 Typically, closed-loop stored value would not include a product that had functionality enabling users to make cash withdrawals or funds transfers, or to obtain a cash redemption of the balance. A product that is otherwise closed loop but permits any required de minimis cash out under state gift card laws should not be deemed open loop by that feature alone.46

Accordingly, an entity that issues or sells open-loop stored value may be subject to state money transmitter laws. With respect to contextual commerce payments transactions, this could include, for example, nonbank entities that issue a stored-value service that can be used in connection with a consumer’s ability to fund (or prefund) payment transactions across a wide variety of digital platforms. An entity

---

42. For example, the state of Washington, in an Interpretive Statement produced by the Department of Financial Institutions, provides that payment processors/payee agents may be exempt from regulation as money transmitters if they meet certain requirements. See Washington Department of Financial Institutions, Interpretive Statement 2015-1, supra note 39.

43. Cal. Fin. Code § 2010(l). “Agent” is defined as “one who represents another, called the principal, in dealings with third persons.” A “payee” is the provider of goods or services, who is owed payment of money or other monetary value from the payor for the goods or services, while the “payor” is the recipient of goods or services, who owes payment of money or monetary value to the payee for the goods or services. See id.


45. See, e.g., Tex. Fin. Code § 151.301(b)(8)(C) (exempting from the definition of “stored value” an electronic record that is “redeemable only for goods or services from a specified merchant or set of affiliated merchants”).

that offers such functionality should be aware of these laws and licensing requirements and appropriately assess applicability.

2. Federal BSA—Money Services Business Requirements

The BSA requires that a “money services business” (MSB), which includes an entity that provides money transmission services, comply with certain registration requirements, customer identification procedures, and transaction monitoring, recordkeeping, and reporting requirements. The regulations implementing the BSA define “money transmission services” in a similar fashion to state licensing laws (i.e., as the acceptance of funds from one person and the transmission of those funds to another location or person by any means). Under the BSA, however, whether an entity is a money transmitter “is a matter of facts and circumstances.”

3. Exemptions from the Definition of Money Transmitter

a. Payment Processor Exemption

The BSA regulations exempt from the definition of “money transmitter” a person that only “[a]cts as a payment processor to facilitate the purchase of, or payment of a bill for, a good or service through a clearance and settlement system by agreement with the creditor or seller” (“payment processor exemption”). The Financial Crimes Enforcement Network (FinCEN), which implements the BSA, explained in the section-by-section analysis accompanying its final rule adding the payment processor exemption that “[a]lthough payment processors may provide a money transmission service, the service is ancillary to their primary business of coordinating payments either from a debtor to a creditor or, if operating at the point of sale, from a purchaser to a merchant.”

Through administrative rulings, FinCEN has established a four-part test for determining whether the payment processor exemption applies to a payment intermediary:

- The entity providing the service must facilitate the purchase of goods or services, or the payment of bills for goods or services (other than money transmission itself)
- The entity must operate through clearance and settlement systems that admit only BSA-regulated financial institutions

---

47. 31 U.S.C. § 5311 et seq.
49. Id. § 1010.100(ff)(5)(i)(A).
50. Id. § 1010.100(ff)(5)(ii).
51. Id. § 1010.100(ff)(5)(ii)(B).
The entity must provide the service pursuant to a formal agreement
The entity’s agreement must be at a minimum with the seller or creditor that provided the goods or services and receives the funds

b. Integral to the Provision of Services Exemption
In addition to the payment processor exemption, the BSA definition of money transmitter excludes a person that “[a]ccepts and transmits funds only integral to the sale of goods or the provision of services, other than money transmission services, by the person who is accepting and transmitting the funds.”\(^{54}\) FinCEN explains that this provision is intended to address instances in which the acceptance and transmission of funds by a particular entity is “an integral part of the execution and settlement of a transaction other than the funds transmission or transfer” provided by that entity.\(^{55}\) In determining whether the money transmission is integral to the provision of a service, and thus eligible for exemption, FinCEN has set forth three “fundamental conditions” that must be met:

1. The money transmission component must be part of the provision of goods or services distinct from money transmission itself
2. The exemption can only be claimed by the person that is engaged in the provision of goods or services distinct from money transmission
3. The money transmission component must be integral (that is, necessary) for the provision of the goods or services\(^{56}\)

Accordingly, to the extent that an entity accepts funds from one person/entity and then transmits those funds to another location or person/entity by any means, there is a possibility that such entity, outside of applicable exemptions, may be subject to federal MSB registration and BSA compliance. With respect to contextual commerce payments transactions, this could include, for example, nonbank entities that receive settlement funds prior to settling such funds to a merchant. Nonbank payment entities performing similar activities should be aware of these laws and licensing requirements and assess potential applicability.

B. FinCEN Prepaid Access Rule
In 2011, FinCEN published the final Prepaid Access Rule, implementing its delegated authority to regulate “prepaid access” under the BSA.\(^{57}\) The Prepaid Access Rule imposes BSA obligations on “providers of prepaid access” and “sellers of prepaid access”—two categories of MSBs. The Prepaid Access Rule exempts from coverage as an MSB certain categories of prepaid access products and services—including

\(^{54}\) 31 C.F.R. § 1010.100(ff)(5)(ii)(F).
closed-loop products—that, in FinCEN’s view, generally pose lower risks of money laundering and terrorist financing.

Under the Prepaid Access Rule, “prepaid access” is defined as “[a]ccess to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number.” Interpretive guidance from FinCEN suggests that an online account that operates “like a fungible payment instrument in traditional commerce, usable at any number of as-yet-unidentified merchants” meets the definition of “prepaid access” even if there is no separate electronic device such as a physical card associated with the account.

Even if an arrangement involves prepaid access, whether an entity is a provider of prepaid access, and thereby subject to the Prepaid Access Rule, depends on whether the entity (1) has “principal oversight and control” over (2) a “prepaid program.”

- provides access solely to funds not to exceed $1,000 maximum value and from which no more than $1,000 maximum value can be initially or subsequently loaded, used, or withdrawn on any day; and
- does not permit (1) transfers of prepaid access funds between or among users; (2) reloads from a non-depository source; or (3) international transfers.

If an arrangement does constitute a prepaid program, a “provider of prepaid access” is the “participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants.” If no participant in the program is designated the “provider of prepaid access,” determining which participant in a prepaid program has principal oversight and control “is a matter of facts and circumstances.” Activities that indicate principal oversight and control include: organizing the prepaid program; setting the terms and conditions of the prepaid program and determining that the terms have not been exceeded; determining the other businesses that participate in the prepaid program, which may include the issuing bank, the payment processor, or the distributor; controlling or directing the appropriate party to initiate, freeze, or terminate prepaid access; and engaging in activity that demonstrates oversight and control of the prepaid program. (FinCEN subsequently clarified, however, that for a bank-controlled prepaid

---

58. 31 C.F.R. § 1010.100(ww).
60. 31 C.F.R. § 1010.100(ff)(4)(ii).
61. Id. § 1010.100(ff)(4)(iii)(D)(1)(i), (D)(2).
62. Id. § 1010.100(ff)(4)(i).
63. Id. § 1010.100(ff)(4)(ii)(A)–(E).
access program, no entity would be required to register as a provider of prepaid access if the bank has principal oversight and control over the prepaid program.64)

A participant that is determined to be a “provider of prepaid access” would be regulated as an MSB under FinCEN’s BSA regulations. As an MSB, the “provider of prepaid access” would be subject to compliance obligations, including:

- Registering with FinCEN as an MSB and submitting, as part of its registration and registration renewals, a complete list of the prepaid programs for which it serves as provider65
- Reporting transactions in currency in amounts greater than $10,00066
- Reporting on transactions of $2,000 or more that it determines to be suspicious67
- Establishing procedures to verify the identity of a person who obtains prepaid access under a prepaid program68
- Obtaining identifying information concerning such a person, including name, date of birth, address, and identification number69
- Retaining access to such identifying information for five years after the last use of the prepaid access70

A seller of prepaid access is a person that “receives funds or the value of funds in exchange for an initial loading or subsequent loading of prepaid access” if the prepaid access is sold under a prepaid program and can be used before customer information is verified.71 In other words, if the “prepaid access” product is part of a prepaid program, and the provider of prepaid access does not verify the customer’s identity as described above, then the entity selling the prepaid access would be subject to the BSA as an MSB and required to collect and verify identifying information in its own right.72

Accordingly, any entity that issues or sells prepaid access, as defined above, may be subject to regulation as a federal MSB. With respect to contextual commerce payments transactions, this could represent, for example, a nonbank entity operating as a provider or seller of prepaid access (as defined above) that could be used in connection with a consumer’s ability to fund payment transactions across a wide

64. See FinCEN Ruling FIN-2012-R003, Application of the Prepaid Access Rule to Bank-Controlled Programs (June 8, 2012).
65. 31 C.F.R. § 1022.380(a)(1).
66. Id. § 1010.311.
67. Id. § 1022.320(a)(2).
68. Id. § 1022.210(d)(1)(i).
69. Id. § 1022.210(d)(1)(iv).
70. Id. Certain of the above-listed requirements are incremental to the BSA compliance requirements to which an entity would be subject as a money transmitter.
71. 31 C.F.R. § 1010.100(ff)(7).
72. An entity is also a seller of prepaid access if it sells prepaid access (open or closed loop, and regardless of whether part of a prepaid program or not) to funds “that exceed $10,000 to any person during any one day, and has not implemented policies and procedures reasonably adapted to prevent such a sale.” See id. § 1010.100(ff)(7)(ii).
variety of digital platforms. Any entity offering such functionality should be aware of these requirements to appropriately assess applicability.

C. Consumer Financial Protection Bureau Prepaid Accounts Rule

The Consumer Financial Protection Bureau’s (CFPB’s) final rule regulating prepaid accounts (Prepaid Accounts Rule) amends the CFPB’s Regulation E, which implements the Electronic Fund Transfer Act (EFTA), and Regulation Z, which implements the Truth in Lending Act (TILA). In general, the Prepaid Accounts Rule extends a modified version of the regulatory compliance regime currently applicable to payroll card accounts (i.e., Reg E “Lite”) to “prepaid accounts,” including by providing an alternative to requiring written periodic statements, modified error resolution procedures, limited initial disclosures and an annual error resolution notice, and limitations on cardholder liability. The Prepaid Accounts Rule requires certain preacquisition disclosures and extends modified versions of certain requirements of the Credit Card Accountability Responsibility and Disclosure Act to prepaid accounts, including account agreement submission and posting requirements and certain statement disclosures.

I. Scope of the Prepaid Accounts Rule

The Prepaid Accounts Rule amends Regulation E to include “prepaid accounts” as one type of “account” subject to Regulation E. There are two relevant prongs of the “prepaid account” definition.

The first relevant prong of the prepaid account definition (the “marketed or labeled prong”) applies to an account (1) that is marketed or labeled as “prepaid”; and (2) that is redeemable upon presentation at multiple, unaffiliated merchants for goods or services, or are usable at automated teller machines (ATMs). The official staff interpretations of the Prepaid Accounts Rule (the Commentary) provide that

73. The Prepaid Accounts Rule was scheduled to take effect, with certain exceptions, on Oct. 1, 2017; however, on Mar. 15, 2017, the Consumer Financial Protection Bureau published a proposed rule to delay the effective date of the rule. Prepaid Accounts under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z); Delay of Effective Date, 82 Fed. Reg. 13,782 (proposed Mar. 15, 2017). On Apr. 20, 2017, the CFPB released a final rule delaying the effective date of the Prepaid Accounts Rule, as proposed, to Apr. 1, 2018. 82 Fed. Reg. 18,975 (Apr. 25, 2017) [hereinafter Release].

74. See 15 U.S.C. § 1693 et seq. (EFTA) and § 1601 et seq. (TILA); 12 C.F.R. pts. 1005 (Regulation E) and 1026 (Regulation Z). The final rule was issued on Oct. 5, 2016. Prepaid Accounts under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), 81 Fed. Reg. 83,934 (Nov. 22, 2016).


76. For the sake of simplicity, in this section on the CFPB’s prepaid accounts rule, references are made to issuers, rather than financial institutions. The amendments to Regulation E will, however, be imposed on “financial institutions,” which include any “person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services.” 12 C.F.R. § 1005.2(i).

77. Prepaid accounts also include payroll card accounts and government benefit accounts currently subject to Regulation E.
“marketed or labeled as ‘prepaid’” means “promoting or advertising” an account using the term “prepaid.”78 Essentially, if an issuer calls a product “prepaid,” it is a prepaid account under the marketed or labeled prong.

The second relevant prong of the prepaid account definition (the “functional prong”) applies to an account (1) that is issued on a prepaid basis or capable of being loaded with funds; (2) whose “primary function” is to conduct transactions with multiple, unaffiliated merchants or at ATMs, or to conduct peer-to-peer (P2P) transfers; and (3) that is not a checking account, share draft account, or negotiable order of withdrawal (NOW) account.

For participants facilitating contextual commerce payments, it is worth noting that prepaid accounts are not limited to traditional physical cards. While the Prepaid Accounts Rule will not apply in the context of a mobile or digital wallet that only stores a consumer’s payments credentials (i.e., card on file) in order to facilitate payments transactions via a wide variety of digital platforms, the Prepaid Accounts Rule will apply to the extent that a mobile or digital wallet is capable of storing funds.79 Moreover, it appears that the entire wallet would be subject to the Prepaid Accounts Rule if only a portion of the wallet can store funds. Therefore, as of the writing of this chapter, in situations in which an entity issues a mobile or digital wallet for purposes of facilitating contextual commerce payments transactions and the mobile or digital wallet stores both (1) payment credentials of consumers (i.e., card on file) and (2) prepaid funds, but the consumer does not use the stored value functionality of the wallet, the Prepaid Accounts Rule would nonetheless apply.

However, on April 20, 2017, the CFPB released a follow-on final rule concerning a delay in the effective date of the Prepaid Account Rule80 but also noted that it would revisit “the linking of credit cards into digital wallets that are capable of storing funds.”81 As of the time of this writing it is unclear as to how the CFPB will address the applicability of the Prepaid Accounts Rule to situations described above in which a digital wallet has the capability of storing both payments credentials and funds, but the consumer does not use the stored value functionality of the wallet. Given the regulatory implications for contextual commerce participants that issue digital wallets capable of storing payments credentials and funds for the use across a wide variety of digital platforms, this issue will remain a significant concern and should be closely monitored.

78. See cmt. 1005.2(b)(3)(i)–3 (stating, as an example, that a prepaid account would be marketed or labeled as prepaid if the term “prepaid” appeared on the access device or on the packaging materials of the access device, or on a display, advertisement, or other publication to promote purchase or use of the account).
79. A digital wallet that only stores a consumer’s payment credentials is not covered, provided that the digital wallet is incapable of storing funds.
80. Release, supra note 73.
81. Id. at 18,977.
D. Compliance with PCI DSS

Given the number of participants in a contextual commerce payments transaction that potentially can encounter consumer payments credentials, the application of and compliance with the PCI DSS is of paramount concern. Importantly, payment processors, merchants, and any other entity that stores, processes, or transmits cardholder data as part of a contextual commerce payments transaction must comply with PCI DSS.82 PCI DSS identifies the requirements applicable to securing cardholder information, including technical security standards, access controls, monitoring functions, and governance policies.83 The Payment Card Industry Security Standards Council, which was established by the payment card associations, administers PCI DSS and specifies the controls and steps that entities must take to verify or report on their compliance with the standard.84

As founding members of the Payment Card Industry Security Standards Council, the payment card networks enforce compliance with PCI DSS, either directly for member banks, or indirectly through member banks for payment processors, merchants, and other entities that store, process, or transmit cardholder data in the card processing value chain.85 Member banks typically include compliance with PCI DSS as a requirement in contracts with other payment processing participants, or otherwise require compliance with the card association rules, which in turn mandate PCI DSS compliance. Thus, PCI DSS is, most directly, a contractual requirement.

PCI DSS compliance is not mandated by federal law, but three states have mandated compliance with PCI DSS, at least in part. Nevada goes furthest in mandating compliance with the standard for any company doing business in the state that collects payment card information in connection with the sale of goods or services.86 Washington exempts “processors, businesses, and vendors” from certain data breach liabilities if these entities are certified compliant with the current version of PCI DSS at the time of the breach.87 Minnesota incorporated into state law one aspect of PCI DSS—a prohibition against storing the card verification value, personal identification number (PIN), or full magnetic stripe data.88 As a result, noncompliance with PCI DSS can not only result in a contractual breach, but can also violate certain state laws.

Noncompliance with PCI DSS also can be a factor in litigation in determining whether a breached company implemented reasonable security safeguards to protect cardholder data. Merchants and other companies where payment card data was

---

83. See id. for an overview of PCI DSS.
88. See Minn. Rev. Stat. § 325E.64 subd. 2.
accessed without authorization from the companies’ systems have been subjected to lawsuits by companies that allegedly suffered damages from the breach, such as card-issuing banks. In some of these cases, plaintiffs have alleged that the defendant company that suffered the breach was negligent because, among other things, the defendant company was not in compliance with PCI DSS.89

III. CONCLUSION

Given the recent history of contextual commerce as viewed through the lens of merchant and digital platform experimentation with buy-button technology and other similar attempts to move commerce to consumers, it might be easy to discount the impact of contextual commerce based on indicators of poor consumer response. After all, while the idea of taking commerce to consumers wherever they may be makes perfect sense on paper, it is also obvious that consumers need to be willing and able to make purchases when presented with the opportunity.

Of course, issues pertaining to whether consumers will be “willing” to make a purchase outside of what the consumer considers to be an appropriate purchase channel are beyond the scope of this chapter. Issues pertaining to whether consumers are “able” to make the purchase, however, are largely within the ability of contextual commerce stakeholders to control and, as pointed out in the introduction to this chapter, may be positively influenced through further reductions in payments friction via solutions that limit the need for consumer interaction with the payment process.

In order to provide that kind of functionality, it is likely that providers will need to implement end-to-end contextual commerce solutions, including (1) the maintenance of relationships with digital platforms that utilize the provider’s contextual commerce solution; (2) the maintenance of relationships with merchants looking to transact on a wide variety of digital platforms; and (3) the ability to provide payment services to consumers via digital wallets and/or stored value that will either fund or facilitate the funding of merchant transactions that occur via the participating digital platform. In doing so, the contextual commerce provider will be able to orchestrate, at least in theory, the type of “invisible” payments process that has been so successful in other contexts.

It is, however, this positioning as the conduit through which contextual commerce payments transactions occur that brings to bear many of the legal issues discussed in this chapter. And while each of these legal and regulatory issues might be applicable today depending upon the structure of the contextual commerce solution, the evolving nature of the payments industry as well as the legal landscape will trigger the possibility of further regulatory obligations. As a result, contextual commerce stakeholders—whether merchants, payments processors, digital platforms, or others—may benefit from the advice of legal counsel concerning the impact of these and future developments.